

# DESIGNING ACTIVE DIRECTORY FOR SECURITY

**After reading this chapter and completing the exercises  
you will be able to:**

- ◆ Identify and explain the need for various Active Directory Components such as domains, trees, forests, and organizational units.
- ◆ Design an effective and secure Organizational Unit structure.
- ◆ Identify the reasons for using single or multiple domains or multiple forests in Active Directory, and the security implications of each model.
- ◆ Design and implement security templates using the Security Configuration Tool Set.
- ◆ Design and implement effective Account Policies for the domain.
- ◆ Understand the rationale and procedures for delegating control of administrative tasks to users or groups.
- ◆ Understand the various security groups available in Active Directory.
- ◆ Understand how Group Policy can be used to configure and implement an effective security plan.

**A**n essential component to designing an effective security strategy for a Windows 2000-based network is a thorough understanding of Active Directory. **Active Directory** is the directory service on a Windows 2000 network, and it includes all of the user objects, group objects, and computer objects that are used to assign permissions to network resources. The Active Directory configuration has a direct effect on the security plan. At the top level, the design of the domain structure, including the number of domains and the relationships between domains, will influence how you design the security solution. The implementation and management of users, groups, and resources is an important part of the security plan. Even securing Active Directory itself, by controlling who has permission to change the Active Directory objects, must be included in your plan. Active Directory includes several tools to make the management of security easier, including Group Policies and security templates.

This chapter introduces the Active Directory components that you need to work with when you make security decisions for your corporation. Concepts related to forest, domain, and organizational unit design are discussed to ensure the best strategy when developing and implementing a security plan. New features such as security templates, administrative delegation, and Group Policies are illustrated to show the potential that Windows 2000 provides for advanced security configuration.

---

## ACTIVE DIRECTORY COMPONENTS

Active Directory is Microsoft's implementation of a directory service for a Windows 2000 network. A **directory service** is a central database that stores information about network objects such as computers, printers, users, and groups. Active Directory acts as the central authority for network security. Whenever any security principal tries to access network resources, Active Directory must first authenticate the security principal before access to the resources is granted based on the authentication. Active Directory also enables the central administration of directory information. The single database means that the administrator can work with all of the network objects in a single location to assist in object management and security. The final component of a directory service is that it provides information to clients of the directory. For example, you can store the office phone numbers for all of your users in Active Directory so that users on the network can use the directory to search for this information.

Active Directory is organized in a hierarchical structure consisting of a variety of objects. These objects can be organized into logical groups and placed within container objects to allow for easy management. For example, if a company included two locations such as Winnipeg and Vancouver, then these two containers would be created in Active Directory. Any user objects for people who worked in Winnipeg would be placed in the Winnipeg container, and any user objects that belonged in Vancouver would be placed in the Vancouver container. Administrators could then assign specific and distinct administrative policies to these two containers, which would then be applied to the objects in the container.

The **Active Directory schema** defines every object and every attribute available to objects. The schema is essentially a set of rules that defines what types of objects you can create, what types of attributes are required for the object, and what attributes are optional. The types of objects that you can create are called class objects. One example of a class object is a user object. When you create a user object, you have to define some attributes or properties such as the logon name. Other attributes, such as address information, are optional. The Active Directory schema is extensible, which means that you can add new classes or attributes to the schema.



The directory information is stored in a database named `ntds.dit`, which is stored by default in the `systemroot\ntds` folder. This database is located on all domain controllers.

## Active Directory Domains

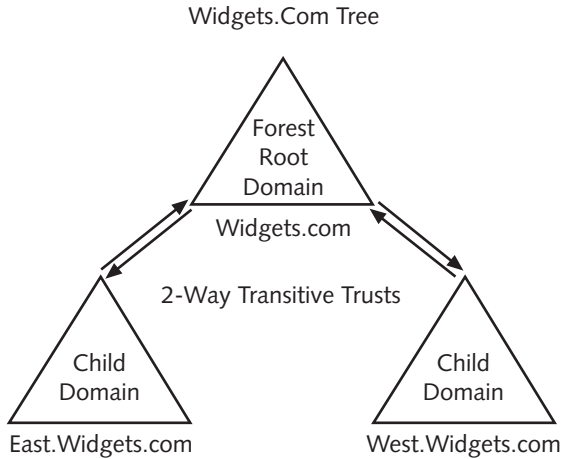
Active Directory domains are the core units of the Windows 2000 logical network structure. A **domain** is a collection of objects that are linked together by the fact that all of the objects are included in the same domain. The objects in a domain can include security principals (users, groups, and computers), as well as organizational units, distribution groups, printer objects, or file shares. The object information is stored in the domain database on at least one server called a **Domain Controller (DC)**.

A domain forms a security and replication boundary in Active Directory. The security boundary defines the scope of permissions for Active Directory security principals. For example, a member of the Domain Admins group in a domain has complete administrative access to all objects in the domain, but, by default, does not have any access to resources in other domains. The Domain Admins group can be used to assign permissions in another domain if a trust exists, but, by default, the group does not have any administrative rights outside of its domain. The security boundary also defines the boundary for other settings, such as trusts and domain security settings. The replication boundary defines which Domain Controllers get a complete copy of the domain database and other domain information. The entire domain database and the Sysvol folder on each Domain Controller are replicated to every domain controller in a domain, while only some of the information in the domain database is replicated to other domains. Each domain in Active Directory also has a unique name, based on the DNS naming structure.

## Active Directory Trees

Windows 2000 uses DNS names for domain names, which means that Windows 2000 domain names are hierarchical like DNS names. An **Active Directory tree** is a grouping of one or more Windows 2000 domains that share a contiguous DNS naming strategy. This means that all of the domain names in the tree share the same DNS root name. The first domain in the forest is called the **forest root domain**. For example, if the first domain in a forest is called Widgets.com, then other domains in the tree might include West.Widgets.com and East.Widgets.com. Any domain that is higher in the namespace hierarchy is called a **parent domain**, while a domain that is connected to a parent domain is called a **child domain**.

The domains within an Active Directory tree are linked together by a **two-way transitive trust**. This allows resources to be shared between domains, and security principals from one domain can be given access to resources in another domain. The transitive trust means that if two domains trust a third domain, then they will automatically trust each other. For example, as illustrated in Figure 4-1, both East.Widgets.com and West.Widgets.com trust the parent domain, Widgets.com. Because of the transitive trust, the two child domains also trust each other.



**Figure 4-1** Active Directory structure and trusts

Each domain within a tree maintains its own directory objects such as users, groups, and computers, and this information is not replicated to the other domains. A central database called the **global catalog** allows users to authenticate or easily find resources across domains in the same tree or forest. The global catalog includes every object in the entire tree, but only includes a subset of the attributes for each object. For example, every user in the global catalog may have their phone number attribute listed, but the department attribute is not. The global catalog can be compared to a phone book, where the name, phone number, and address of individuals throughout a city may be listed, but this information is only a subset of the information that the phone company has about each person.

This global catalog is stored on a server called the **global catalog server**. The first domain controller in the forest root domain is assigned this role by default. In most cases, you should designate additional Domain Controllers to be global catalog servers.

## Active Directory Forests

A **forest** is a collection of one or more Active Directory domain trees that share a single schema and global catalog, and are connected by two-way transitive trusts. The trees in a forest DO NOT have to follow the same DNS naming hierarchy. This can allow companies that consist of distinctly named divisions to participate in one main Active Directory structure. For example, as illustrated in Figure 4-2, a company may have one tree with a parent domain called Widgets.com and a second tree with a parent domain called MiniWidgets.com.

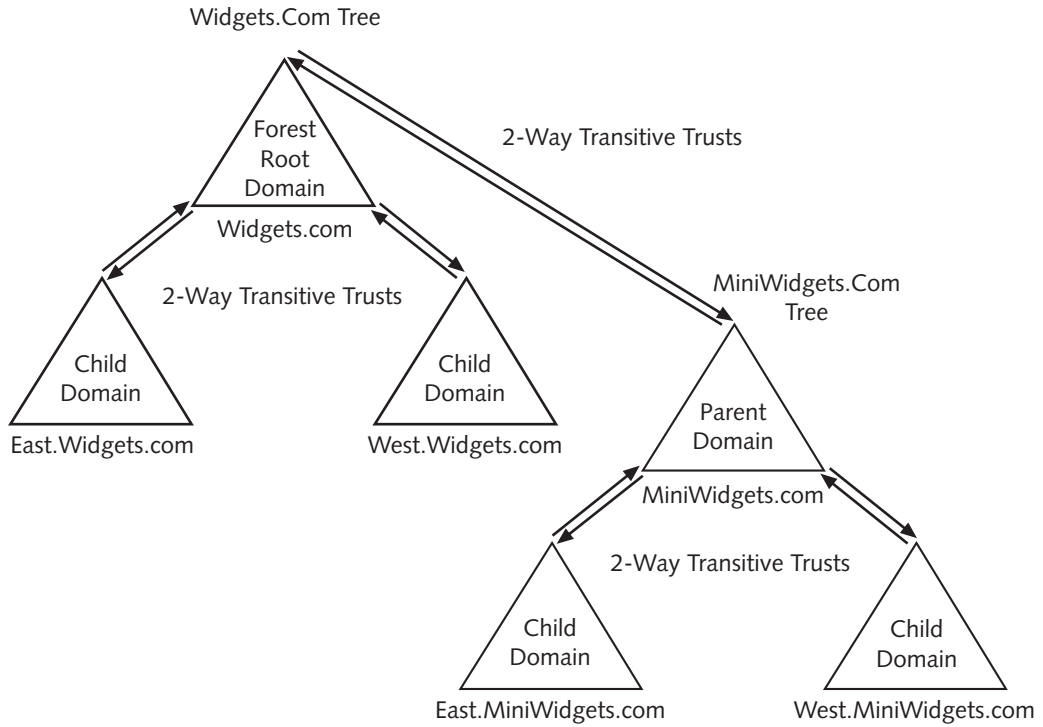


Figure 4-2 Multiple trees in one forest

## Organizational Units

One of the most useful objects in an Active Directory domain is an organizational unit. An **organizational unit (OU)** is a container used in Active Directory to logically group and manage objects such as users, groups, computers, and other OUs. An OU is typically created for each departmental or geographical division within the company. For example, a company may have marketing, finance, and IT divisions. An administrator can create three separate organizational units within an Active Directory domain with the standard division names. The Active Directory objects can then be placed in the corresponding OUs. For example, if John worked for the finance department, the Active Directory administrator would place John's user object and computer object in the Finance organizational unit. Any finance-related user, group, or computer objects would be placed in that OU. The same process would be applied to the Marketing and IT Organizational Units.

OUs are useful in Active Directory because they can be used to administer a collection of users or computers as a single unit rather than administering each object separately. For example, if you wanted to install a finance application on all of the computers in the Finance department, and all of the computers were grouped in the Finance OU, you could use a group policy to install the application automatically. Another important

benefit of using OUs is that you can delegate administrative permissions at an OU level. Active Directory gives the administrator the capability to delegate tasks, such as resetting passwords or adding user accounts, at an OU level, without giving the delegate any other administrative rights in that OU or anywhere else in the domain. Administrative tasks such as delegation will be discussed later in the chapter.

When planning the organizational unit structure for an organization, you should follow a few general guidelines:

- Avoid creating an OU structure that contains too many levels of OUs nested inside other OUs. The maximum number of OU levels should never exceed 10 levels, and search performance is adversely affected when the OU levels reach five. If you find yourself needing more OU levels than is recommended, look at the option of creating additional domains or try to reorganize the OU plan.
- Verify that the OU structure you develop is relatively stable, even if the company should reorganize. This is especially important for the OUs higher up in the hierarchy. This may mean that OUs based on geography are more appropriate at the top of the OU structure than OUs based on job function, because the job function is more likely to change than the geographic structure of the company.
- Organizational units are not security principals. This means that you cannot assign permissions to an OU and then have all of the users in the OU automatically inherit those permissions. OUs are intended to give users or groups rights or permissions to objects inside the OU; OUs are not intended to give permissions elsewhere in the domain.

## Sites

All of the Active Directory concepts discussed so far are logical concepts that are quite independent of the company's geographic locations and the network topology. A company with one location may have multiple domains, while a company with multiple locations may have a single domain. An organizational unit may include all of the users in a particular office, or the OU may include users from several offices scattered throughout the country. The only Active Directory concept that is strongly dependent on the company's physical network is the concept of sites.

A **site** is defined as a group of computers that are connected to each other with a fast network connection. The concept of a site is important in a number of ways. First, when a user logs on to a Windows 2000 computer, the computer will always try to connect to a Domain Controller in the same site as the client. When a client tries to access a distributed file system (DFS) share, the client will always connect to a share in the same site as the client. The concept of sites is also used to manage replication traffic between Domain Controllers. The replication of domain information between Domain Controllers in the same site is not compressed, and the schedule for replication cannot

be controlled. When the two Domain Controllers are in different sites, then the replication traffic is compressed, and the administrator can configure a schedule to indicate when the replication occurs. In every case, the benefit of splitting the company's network into sites is that you can then control the amount of traffic that will be sent across the slower WAN connections between company locations.

## Domain and Forest Design—Security Planning Implications

## 4

Designing the Active Directory structure for a large corporation is a long and complicated process. In most cases, the goal of Active Directory design is to keep the design as simple as possible. Following this principle usually means that most organizations will try to create an Active Directory structure that includes only a single domain. One Active Directory domain can contain over 100,000 objects, so most organizations will not have to implement multiple domains. However, some organizations do need additional domains. A multiple-domain model is usually deployed with companies that require different password and security policies between domains. As mentioned earlier, domains define security boundaries, whereas, by default, a user account in one domain does not have any permissions in a different domain. If an organization requires this distinct security boundary, then it will have to create multiple domains. A domain can only be assigned one default language, and so geographical/language issues may also interfere with the intended single-domain model.

The same principle applies to the question of deploying multiple forests. Most companies will deploy a single forest as opposed to multiple forests. A single forest provides the following advantages:

- Easier forest-wide administration—Users can be given access to resources directly, or belong to groups that may have the ability to be easily assigned across multiple domains within the forest. Multiple forests increase the complexity and may require duplicate groups to be created.
- Secure Kerberos-authenticated trusts—Single forests create two-way Kerberos-authenticated trust relationships between the domains. Multiple forests cannot be configured to actually trust each other. Only single domains between the multiple forests can trust each other, and the trusts are one-way, non-transitive, and use NTLM authentication.

Companies may decide on a multiple-forest design if they are involved in mergers with other companies that already have Active Directory in place. Also, if divisions need separate schema policies, then two separate forests would be needed to meet this requirement.

The most important security implication for Active Directory design at the forest and domain level has to do with the inheritance of administrative rights throughout the organization. When a new Active Directory forest is created by installing the forest root domain, two important security groups result from the creation of the domain. The first group is the Schema Admins group, and the members of this group are the only users

who have the right to make any changes to the Active Directory schema. The second group is the Enterprise Admins group. The Enterprise Admins group is automatically added to the Administrators group in every domain in the forest, which means that the members of the Enterprise Admins group have full administrative rights in every domain in the forest. You can remove the Enterprise Admins group from the Administrators group in a domain, but a member of the Enterprise Admins group can always add the group back into the Administrators group. The permissions inheritance by the Enterprise Admins group is the only exception to the concept that a domain forms a security boundary. The security boundary does not prevent the Enterprise Admins group from having permissions throughout the forest. The Schema Admins group and the Enterprise Admins group are created only in the forest root domain and, by default, the administrator account that was used to create the forest root domain is the only member of these groups.

Because of the rights granted to these two groups, they create a special security concern. An essential part of your security plan will be to define and limit the membership of these groups. As well, your security plan should include an audit policy for any actions taken by the members of these groups. In some corporations, the concept of the Enterprise Admins group having complete access to all domains in the forest may be unacceptable, and your security plan may require multiple forests to ensure that no account has administrative rights to every domain in the organization.

A similar security issue arises from the role of the Domain Admins group in a domain. The Domain Admins group has complete administrative control of the entire domain, including every OU. In some organizations, the OU structure is used to separate administrative units so that separate groups of administrators have control over different OUs. By default, the Domain Admins group has administrative rights to every OU. The OU administrators can remove the Domain Admins group from having administrative rights at the OU level, but a member of the Domain Admins group can always reassign the administrative rights. If this situation is unacceptable in your organization, then your security plan will need to include the implementation of multiple domains. By default, the Domain Admins group in one domain has no administrative rights in any other domain.

---

## SECURING ACTIVE DIRECTORY

In the past, as network systems increased in size and complexity, administering security across the enterprise also became increasingly complex. Windows NT did not provide adequate tools or utilities to implement and manage an effective network security policy. For example, if an administrator wanted to implement security auditing on a particular group of workstations, either she would have to visit each machine individually or try to find adequate third-party tools to assist in the configuration.

Another common problem with managing security policies in Windows NT is the maintenance of the configuration. If a company or department has more than one



administrator in charge of applying and maintaining the security settings, it can be difficult to keep track of configuration changes to the policy. Without proper documentation and good communication between the administrators, a great deal of time may be spent figuring out what auditing and security settings each administrator has changed.

Windows 2000 makes significant changes to how security configurations can be maintained. One of the sets of tools that are included with Windows 2000 is a set of components called the **Security and Configuration tool set**. This tool set, together with Windows 2000 Group Policies, allows an administrator to configure a specific group of security settings to form a **Security Policy Template**. This template can then be administered centrally and applied throughout Active Directory.

To assist with security policy changes, the Security and Configuration tool set can also be used to analyze and implement security settings on a computer system. In the analysis, a comparison can be made between a computer system's security settings and a previously defined security template file. Differences between the computer system and the policy template can then be viewed and reported, and actions can then be taken to change the settings on the computer to the desired settings.

For example, your security plan may provide detailed information on the security settings for the company's computers. Creating the design is only the first step, however. You also need to implement the design, which could mean making changes to every computer on the network. The Security and Configuration tool set is designed to make the implementation of the security policy much easier. When the security policy has been designed and approved, the settings can then be defined in a security template. This template can then be compared to the current settings on the network by using the Security Analysis tool. This will give a clear picture about which current settings match the security policy and which ones do not. You can then apply and implement the new settings with a simple command.

The Security and Configuration tool set is also useful in maintaining the security settings. Using this tool, it is easy to check the security settings for the network on a regular basis and reapply any settings that have been changed.

The Security and Configuration tool set consists of the following components:

- Security Templates
- Security Settings in Group Policy Objects
- Security Configuration and Analysis
- Secedit Command Line tool

## Security Templates

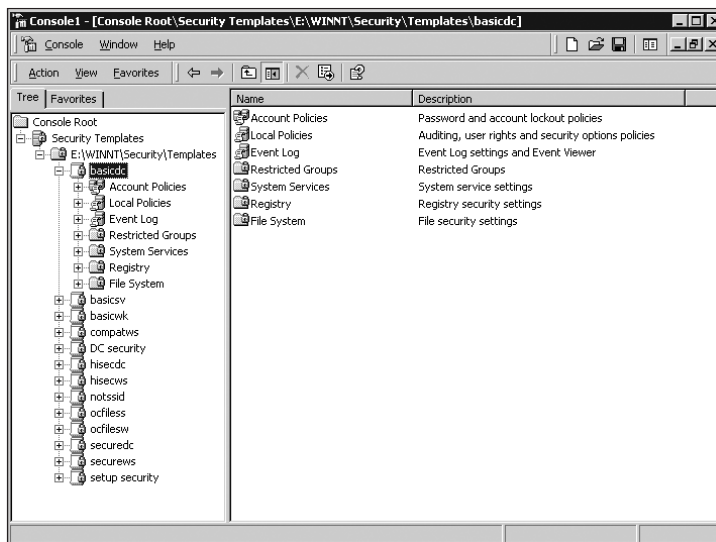
An administrator uses security templates to define, edit, and save baseline security settings to be applied to computers with common security requirements. Templates help ensure that a consistent setting can be applied to multiple machines and easily maintained.



The templates are text-based files that can be read, but should not be changed or edited using any text editor. Be sure to use the Security Templates snap-in to create and edit the templates.

Security settings can be defined by loading the Security Templates snap-in on the Microsoft Management Console (MMC). To load the snap-in, follow the steps below:

1. Click **Start** and click **Run**.
2. Type **mmc** in the Run command line. An empty MMC will appear. You may want to maximize the console.
3. Click the **Console** menu and click **Add/Remove Snap-in**.
4. Click the **Add** button.
5. In the Add Standalone Snap-in dialog box, scroll down and click **Security Templates**, and then click the **Add** button.
6. Click **Close**, and then click **OK**.
7. Click the **Plus sign** next to Security Templates in the leftmost pane.
8. The next node will show you the physical location of the security template files on the server. The location of the template files is usually `c:\%systemroot%\security\templates`.
9. Save the new MMC by clicking the **File** menu and clicking **Save As**. Choose an appropriate name and location for the MMC console file.



**Figure 4-3** Security Templates snap-in loaded into the MMC

Security templates include the following seven main security categories:

- **Account Policy**—This category consists of settings used to define account authentication and user password settings. There are three sub-categories that can be configured:
  - **Password Policy**—Includes settings related to password history, length, and high-complexity requirements.
  - **Account Lockout Policy**—Allows administrators to set the amount of tries that are accepted before locking out logon attempts. Settings are also available for configuring the duration of the lockout.
  - **Kerberos Policy**—Includes various Kerberos-related settings such as session and TGT ticket lifetime and maximum clock deviance.



When Account Policies are assigned to Active Directory using Group Policy, make sure to assign this level of policy to a Domain Group Policy Object. This will apply the policy to all of the domain members. If you assign the policy to any other OU, it will affect only the local account database on the member server or workstation. This is especially important regarding the Password Policy category.

- **Local Policy**—This category applies security settings to the local account database of the workstation or server. These may be overwritten at the site, domain, or OU level, but will remain in effect if there are no other policies at those levels. There are three subcategories that can be configured:
  - **Audit Policy**—Defines various successful or unsuccessful events that can be audited and recorded in the event logs. See Chapter 3, “Securing Resources on Windows 2000 Servers” for information regarding these events.
  - **User Rights Assignment**—Controls local computer rights that may be assigned to users or groups. For example, the right to log on locally, or to shut down the computer.
  - **Security Options**—Defines a wide variety of configuration settings that will adjust the registry. Some examples include restricting floppy or CD-ROM access, logon banner configurations, and removing the last logged-on user name from the logon screen.
- **Event Log**—Defines configuration settings in relation to event log size, retention period, and access restrictions.
- **Restricted Groups**—This category gives the administrator the ability to control who is a member of any security group. Each time that the policy is refreshed, any users that have been added to the group by any means other than the security template will be removed automatically. This category can also control what other groups a particular security group belongs to.

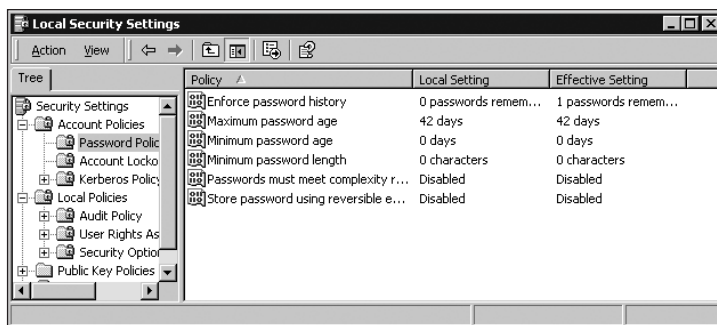
- **System Services**—This category allows an administrator control over configuring service startup mode, disabling a service, assigning permissions to edit the service mode, and auditing of the service.
- **Registry**—Defines security and auditing ACL settings for Registry keys and subkeys. This allows an administrator to control who has access and the right to change or overwrite registry settings.
- **File System**—Defines and maintains security permissions (DACL) and Auditing permissions (SACL) for any folder or file listed in the policy. Files or folders must reside on an NTFS partition.

## Applying Security Templates

Security templates can be applied to either the local machine, or to the domain through Group Policy Objects. To apply a security template to a local machine, follow the steps below:

1. Click the **Local Security Policy** from the Administrative Tools menu.
2. Right-click **Security Settings** in the left pane and click **Import Policy**.
3. Select the template file to be imported and click **OK**.

In the Local Security Settings MMC, there are two columns: one that displays local settings, and one that displays effective settings, as shown in Figure 4-4. Local settings are the settings that are applied to the local computer. Effective settings indicate that there are domain-level or OU-level security settings applied for that particular policy. The settings that are applied at a domain or OU level will always override the local settings. Domain-level security settings are applied any time the machine is rebooted, and at 90-minute intervals if changes have been made to the policy. If there have been no changes, the domain policy is refreshed every 16 hours.



**Figure 4-4** Local and effective security settings

To apply security templates to Active Directory using Group Policy, follow the steps below:

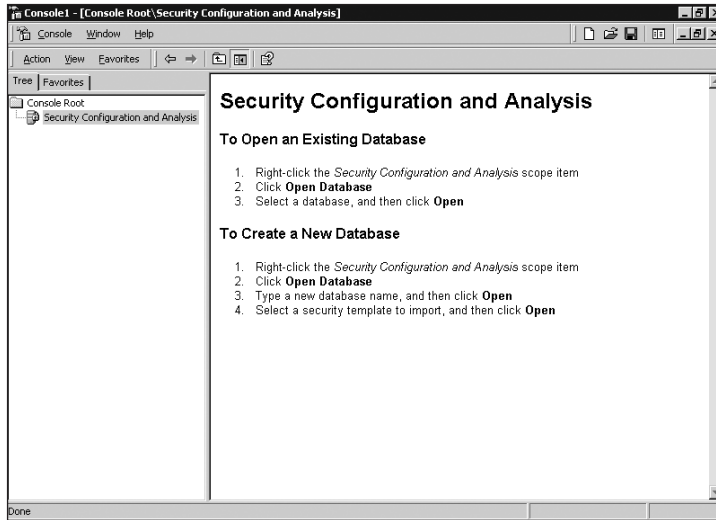
1. Click **Active Directory Users and Computers**.
2. Right-click the node that is to have the security settings applied and click **Properties**. If the security settings refer to the Account Policies, be sure to apply this template to the Domain Controllers OU.
3. Click the **Group Policy** tab and click **New** or **Edit**, depending on whether there is already a Group Policy that can be edited.
4. Under **Computer Configuration**, click **Windows Settings**, and expand the **Security Settings** node.
5. Right-click the **Security Settings** node and click **Import Policy**.
6. Select the appropriate policy to import and click **Open**.

## Security Configuration and Analysis

The Security Configuration and Analysis utility allows administrators to compare current system settings to a previously configured security template. The comparison identifies any changes to the original security configurations, as well as any possible security weaknesses that may be evident when compared to a stronger security baseline template.

In order to perform a security analysis, the Security Configuration and Analysis snap-in must be loaded into a Microsoft Management Console shell. To load the snap-in follow the directions below:

1. Click **Start** and click **Run**.
2. Type **mmc** in the Run command line. An empty MMC will appear. You may want to maximize the console.
3. Click the **Console** menu and click **Add/Remove Snap-in**.
4. Click the **Add** button.
5. In the Add Standalone Snap-in dialog box, scroll down and click **Security Configuration and Analysis**, and then click the **Add** button.
6. Click **Close**, and then click **OK**. See Figure 4-5.

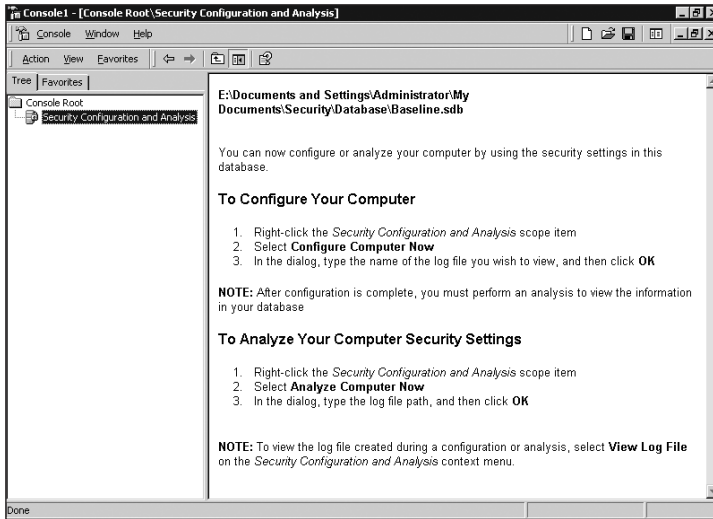


**Figure 4-5** The Security Configuration and Analysis utility

The Security Configuration and Analysis tool uses a container, called a database, to store the imported templates to be compared to the working system. The administrator imports a template into the database and then compares the template settings to the actual computer settings. If desired, the administrator can import more than one template to compare the effects of combining templates on the current settings. Once a combined template has been created, it can be saved and exported for future analysis, or it can be used to configure working computer systems.

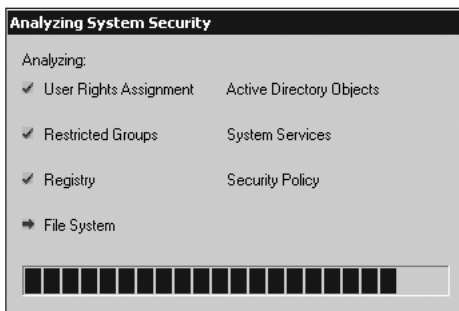
To create the database and perform the analysis, follow the steps below:

1. In the Security Configuration and Analysis MMC, right-click the **Security Configuration and Analysis** node and click **Open Database**.
2. Type a name for the database and click **Open**.
3. Select the security template to import into the database. If the database is being reused, select the **Clear this database before importing** check box. Figure 4-6 shows the interface after you have imported the security template.



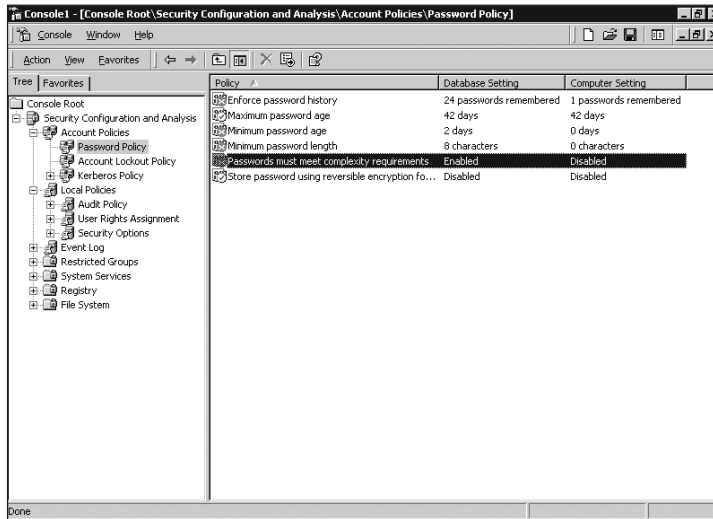
**Figure 4-6** Security Analysis configuration screen

4. To compare the security template to the current computer settings, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.
5. An error log path appears to allow an error log to be saved at a particular location on the computer. Specify a path, a name, and then click **OK**.
6. A progress meter will appear as the analysis takes place. See Figure 4-7.



**Figure 4-7** Security Analysis progress meter

7. After the analysis, the security categories will appear. As each node is expanded, you can see the comparison between the database (imported templates) and the computer's current configuration. See Figure 4-8. A green check mark indicates that the two settings match; a red X indicates a mismatch. You can make changes by double-clicking any configuration entry and selecting the configuration desired.



**Figure 4-8** Security Analysis results

8. If you want to apply the database setting to the computer, right-click **Security Configuration and Analysis** and click **Configure Computer Now**. If you do this, the computer settings will be modified to match the settings in the template.
9. If you want to reuse the template that you have modified, you can export the template by choosing **Export Template** and creating a filename for the new template. The new template can then be deployed using Windows 2000 Group Policy.

## Secedit Command Line Tool

**Secedit.exe** is a command-line tool used to create and apply security templates, as well as analyze security settings. This tool can be used in situations where group policy cannot be applied, such as in workgroup configurations. Secedit.exe, along with the Task Scheduler, can ensure that every computer in the workgroup maintains consistent security policy settings. The secedit.exe command uses five main switches:

- /analyze—Analyzes database settings and compares them to a computer configuration.
- /configure—Configures a system with database and template settings.
- /export—Exports database information to a template file.
- /refreshpolicy—Triggers group policy propagation.
- /validate—Verifies the syntax of a template.





For more information on secdit.exe, consult Windows help.

## MANAGING ACCOUNT POLICIES

One security category that deserves additional attention is the Account Policies node. This node includes configuration settings that may be the initial step to securing the computer network. The Account Policy category, as shown in Figure 4-9, includes three subcategories: Password Policy, Account Lockout Policy, and Kerberos Policy.

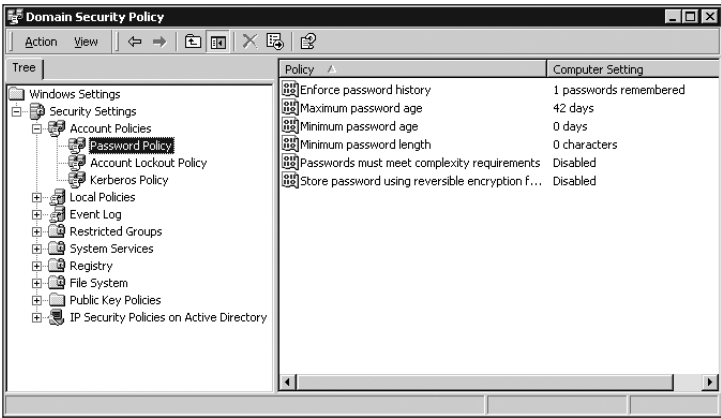


Figure 4-9 Account Policy settings

### Password Policy

The Password Policy node contains configuration settings that refer to the password history, length, and complexity. Table 4-1 describes each setting:

Table 4-1 Password policies in Windows 2000

Configuration Settings	Description
Enforce password history	Defines the number of passwords that have to be unique before a user can reuse an old password.
Maximum password age	Defines the number of days that a password can be used before the user is required to change it. If you never want the passwords to expire, set the number of days to 0 (zero).
Minimum password age	Defines the number of days that a password <b>MUST</b> be used before a user is allowed to change it.
Minimum password length	Defines the least number of characters required in a password. Values can be from 1 to 14 characters. If no password is required, set the value to 0 (zero).
Password complexity requirements	Increases password complexity by enforcing that passwords: <ul style="list-style-type: none"> <li>• Not contain any part of the user's account name</li> <li>• Are at least six characters in length</li> <li>• Contain characters from three of the four categories below: <ul style="list-style-type: none"> <li>- English upper case letters</li> <li>- English lower case letters</li> <li>- Numbers</li> <li>- Nonalphanumeric (!, \$, #)</li> </ul> </li> </ul>
Store password using reversible encryption for all users in the domain	This setting is the same as storing passwords in clear text. This policy provides support for applications which use protocols that need the passwords in clear text for authentication purposes.

## Account Lockout Policy

The Account Lockout Policy node contains configuration settings that refer to the password lockout threshold and duration, as well as reset options. Table 4-2 describes each setting.

Table 4-2 Account Lockout policies

Configuration Settings	Description
Account lockout threshold	Determines the number of failed logon attempts that will result in the user account being locked.
Account lockout duration	Determines the number of minutes that a locked out account remains locked out. After the specified number of minutes, the account will automatically become unlocked. You can specify that an administrator must unlock the account by setting the value to 0 (zero).
Reset account lockout counter after	Determines the number of minutes that must elapse after a single failed logon attempt, before the bad logon counter is reset to 0 (zero).

## Kerberos Policy

The Kerberos Policy node contains configuration settings that refer to the Kerberos Ticket Granting Ticket and session ticket lifetimes, and time stamp settings. Table 4-3 describes each setting.

**Table 4-3** Kerberos Policy Node Configuration

Configuration Settings	Description
Enforce user logon restrictions	Requires the KDC to validate every request for a session ticket against the user rights policy of the target computer. If enforced, there may be a performance degradation on network access.
Maximum lifetime for service ticket	Determines the maximum amount of time, in minutes, that a service ticket is valid to access a resource. Default: 600 minutes (10 hours)
Maximum lifetime for user ticket	Determines the maximum amount of time, in hours, that a ticket granting ticket (TGT) may be used. Default: 10 hours
Maximum lifetime for user ticket renewal	Determines the amount of time, in days, that a user's TGT may be renewed. Default: seven days
Maximum tolerance for computer clock synchronization	Determines the amount of time difference, in minutes, that Kerberos will tolerate between the client machine's clock and the time on the server's clock. Used to prevent "replay attacks." Default: five minutes

Account policies can be implemented on a standalone computer using the Local Security Policy found in the Administrative tools menu. If the computer is a member of a domain, the Account Policies must be set at the Domain Security Policy on a Domain Controller. These settings affect all users and computers in the domain and cannot be applied at the OU level. If a policy is configured at the OU level, it will affect only the local security database of the objects within the OU.

## Account Policies Security Implications

The account policies are an important part of your security plan. In particular, the account policies are a first line of defense against someone trying to get access to your network by guessing the user passwords. There are a number of ways that the account policies can be used to make your network more secure:

- Require long complex passwords. For most networks, a password policy that requires passwords at least 8-10 characters long, and that meets the complexity requirement, is sufficient. In higher security environments, the password length should be increased to 14 characters.

- The account should be locked out after three to five bad logon attempts. Setting this option means that any attempt at brute force password guessing will very quickly result in locked out accounts.
- Require the administrator to unlock user accounts rather than have the account unlock after a certain period of time. If you do not have administrators available to unlock user accounts during the off hours, and you have people who access the network from outside the office, then set the account lockout duration for at least two to four hours.
- Balance the frequency of password changes with the need for password security. If you require long complex passwords, and you require frequent password changes, the chances increase that users will write down their password in a place where it can be found. In most cases, requiring a long complex password and having an account lockout policy is more secure than requiring frequent password changes. For most networks, requiring a password change every 60 days is appropriate.
- Teach the users tricks to memorize long complex passwords. One example is to use a phrase to create the password. For example, “To be or not to be” can become “2BEorNoT2B!”. By using tricks like this, the users can remember complex passwords that are very difficult to break.
- In most cases, the default Kerberos settings do not need to be changed. In a highly secure environment you may want to shorten the key renewal times.

---

## DELEGATING ADMINISTRATIVE TASKS

One of the biggest changes between Windows 2000 Active Directory and the Windows NT domain structure is the ability to delegate administrative tasks in Active Directory. In Windows NT, in order to have any administrative rights in the domain, you have to have a high level of administrative rights throughout the entire domain. In Active Directory, you can assign much more limited administrative rights at the domain level, as well as assign administrative rights to only a part of the domain. In most cases, the delegation of administrative rights is configured at the OU level. In some cases, an administrator may need full administrative rights in a particular OU. In other cases, an administrator may need very limited rights (such as the right to reset passwords) in an OU. Both of these options are easy to implement in Active Directory.

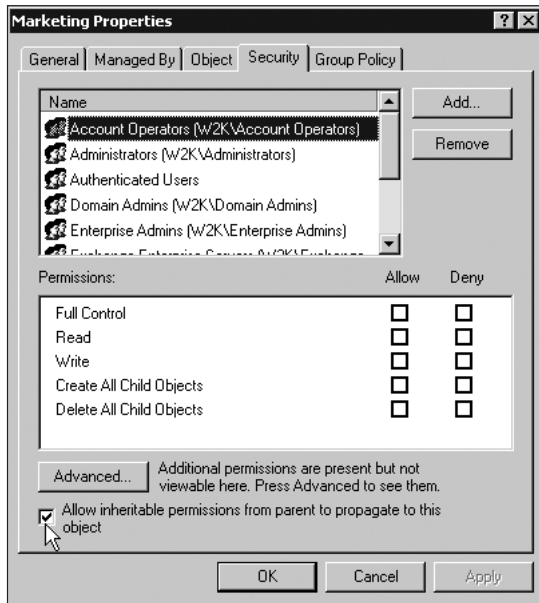
The delegation of administration means that you are configuring the level of access other administrators have to Active Directory objects. As discussed in the last chapter, every object in Active Directory has a discretionary access control list (DACL) that defines the level of access all users have to the object. To ensure proper delegation, you must first understand how these permissions are inherited throughout Active Directory. Administrators must be sure to delegate only the required permissions to users, and understand how those permissions affect child objects of a particular container.

## Permission Inheritance

By default, all child objects inside a container object inherit the permissions from the parent object. By using this inheritance and planning carefully, you can eliminate the need to assign permissions to every container object or to every object inside a container. The permissions are inherited from the parent container when the object is created. If the permissions to the parent container are changed after the child object has been created, the permissions can be forced to the child container by making sure that any change in permissions is inherited by all child objects. You can do this by making sure that This object and all child objects is selected under Advanced on the Security tab of the Active Directory parent container.

This default inheritance of permissions can be modified by blocking the inheritance at a container or object level. For example, you may want to have all of the permissions that are set at an upper-level OU inherited by all child OUs except for one particular child OU. You may want to give the help desk personnel the right to reset the passwords for all of the users at the corporate Head Office OU, except for the executives. In this case, you could put all of the executives in an Executives OU and then accept the default inheritance for all child OUs, but block the inheritance for Executives OU. To override the inheritance of permissions at an OU level, follow these steps:

1. Click **Active Directory Users and Computers**.
2. Browse to the OU where you want to override the inherited permissions and click **Properties**.
3. Click the **Security** tab.
4. To override the inherited permissions, clear the **Allow inheritable permissions from parent to propagate to this object** check box. See Figure 4-10.
5. You are given the choice to copy the inherited permissions and then change them, or to remove all permissions and then assign new permissions.



**Figure 4-10** Modifying the inheritance of permissions at an OU level

## Managing Delegation

The delegation of administration allows you to distribute and decentralize the process of administering Active Directory. To accomplish this goal, the first step is to design the OU structure in such a way that the administration work can be distributed. For example, you may want to assign the task of managing one small part of the network to a junior administrator or an administrator in a remote location. Creating an OU, and then delegating the administrative control to that person, is an ideal solution to accomplish this step.

The second step of delegating the administrative control is to configure the appropriate level of administrative permissions for each administrator. You may want to give another administrator full control of one particular OU, but you may not want that person to have any administrative permissions anywhere else. Again, the option of assigning permissions to specific OUs allows you to achieve this goal.

## Implementing Delegation

You can manage the permissions on every Active Directory object by directly viewing and modifying the DACL on the object. However, this can be a very complicated task, especially if you are delegating a variety of tasks in a complex OU structure.

To make the delegation quicker and easier, Windows 2000 provides the Delegation of Control Wizard. This wizard guides you through the process of determining the permissions that you want to delegate and then configures the DACL for the object and child objects.

In addition to the Delegation of Control Wizard, Windows 2000 provides two other options that make the delegation of administrative permissions easier to implement. The first option allows you to customize all of the administration MMCs so that the delegated administrator can view only the part of the domain that he is responsible for administering. For example, you can create a customized MMC where only one OU is visible, and then give that customized MMC to the OU administrator. The second option is to create a series of taskpads. A taskpad extends the concept of creating a customized MMC even further and can be used to create a custom interface where a user can perform one or more administrative tasks.

To use the Delegation of Control Wizard, follow this procedure:

1. Right-click the container (domain or OU) where you are delegating control and click **Delegate Control**.
2. The Delegation of Control Wizard starts. Click **Next**.
3. You are given the choice to delegate control to particular users or groups. Click **Add**, choose the user or group, and then click **OK**. Click **Next**.
4. You are now given a list of common tasks to delegate. See Figure 4-11. If the task that you are looking for is not on the common task list, click the **Create a custom task to delegate** option to assign different levels of permission to all objects in the container or to the container itself. If you are using one or more common tasks, select the task(s). Click **Next**.



**Figure 4-11** Choosing a task to delegate

5. Review the information about the delegation that you configured and click **Finish**.

6. To confirm that the permissions are configured correctly, right-click the container object for which you assigned permissions and click **Properties**. Click the **Security** tab. The user's name is listed. To see specific permissions, click **Advanced**. You can modify the permissions here if you wish.



If you decide to change the permissions you have granted to a user, you can also run the Delegate Control Wizard again and assign new permissions to the user. The new permissions overwrite all previous permissions.

## Customizing the MMC

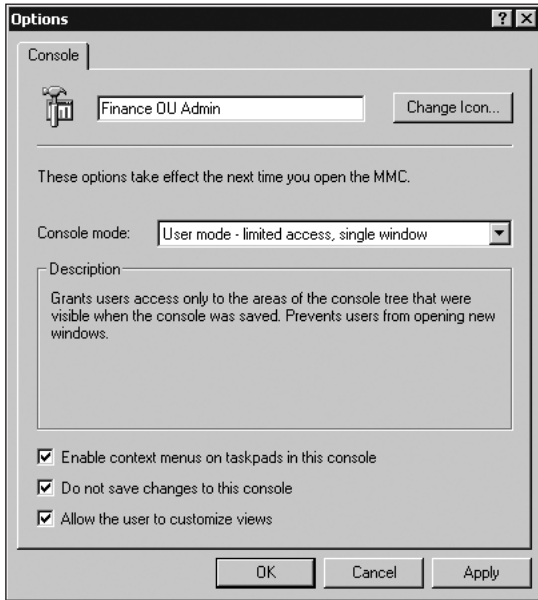
After delegating administrative rights to another user, you can create a custom MMC that limits the view within Active Directory Users and Computers to only the part of the domain that the user has permission to administer. This is particularly useful when the user has been given control over an OU.

If the user who uses the custom MMC is not using a Windows 2000 Domain Controller, the administration tools need to be installed on the computer. The file needed to install the administration tools is called Adminpak.msi and is located on the Windows 2000 Server compact disc.

To create a custom MMC, follow the procedure below:

1. Open a Run command, type **mmc**, and click **OK**. Add the **Active Directory Users and Computers** snap-in to the MMC console.
2. Expand the domain in Active Directory Users and Computers so that the OU with which you are working is visible.
3. Right-click the OU and click **New Window from Here**.
4. To hide the other window that included the entire domain, click **Window** and click **Console 1**. When the Console 1 window is in the foreground, close it. The only window now visible is the view of the OU.
5. To configure the options for the console, click **Console**, and then click **Options**. See Figure 4-12.
  - a. Type a descriptive name for the console.
  - b. Set the console mode to **User mode - limited access, single window**, thus preventing the user from changing the MMC.
  - c. Verify that the **Do not save changes to this console** check box is selected.
  - d. Click **OK**.





**Figure 4-12** Configuring the options on a customized MMC

6. Save the custom MMC.
7. To ensure that the user cannot change the MMC by opening it in author mode from the command prompt or by right-clicking the MMC icon, open the NTFS permissions for the .msc file and remove the user's permission to write to this file.
8. Make the MMC available to the user by e-mailing it to him or her or by putting it on a network share that is accessible to the user. Or, if you have access to the user's profile, save the file or a shortcut to the file on that person's desktop.



By creating a custom MMC in this way, you limit the view that the user has of an OU. This process does not set permissions or delegate authority to the user. You should use the Delegation of Control Wizard to assign permissions.

## Creating and Configuring Taskpads

In some cases, you may need to simplify the administration tools even more than is available through a customized MMC. The taskpad allows you to create a simple management tool that allows a user to perform very specific tasks on a network, while hiding the complexity of the task. The taskpad is designed primarily for users who do not usually perform network administration, but need to perform a simple task such as

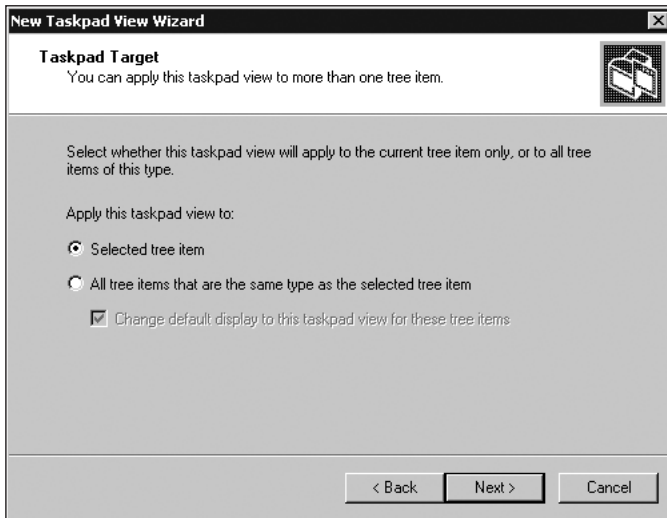
resetting passwords. In the taskpad, each task is assigned to a button, and to perform the task, the user simply clicks the button. To create a taskpad follow the procedure below:

1. Create a custom MMC and add the **Active Directory Users and Computers** snap-in.
2. Right-click the container where you want to create the taskpad and click **New Taskpad View**.
3. The New Taskpad View Wizard starts. Click **Next**.
4. You are given a choice of how the taskpad displays information. See Figure 4-13. Select **Vertical list** for long lists like user accounts or **Horizontal list** to show more information about each item. Click **Next**.



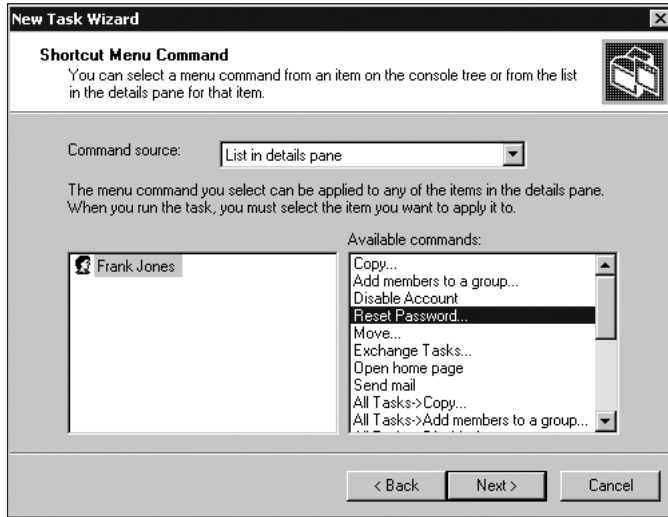
**Figure 4-13** Configuring the Taskpad display options

5. You can now choose whether the taskpad applies to the item you have selected or to other items of the same type. See Figure 4-14. If you are creating this taskpad for a user to administer only one OU, then select the **Selected tree item** option. If you want the user to perform the same task in other OUs (for example, resetting passwords in all OUs), then select the **All tree items that are the same type as the selected tree item** option. Click **Next**.



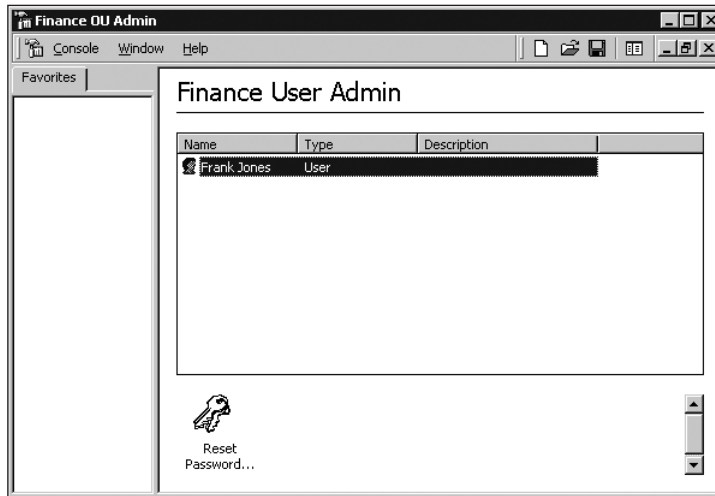
**Figure 4-14** Configuring the Taskpad target

6. Type a name and description for the taskpad. Click **Next**.
7. Now that you have created the taskpad view, you are given the option of assigning tasks to the taskpad. Verify that the **Start New Task Wizard** check box is selected, and click **Finish**.
8. The New Task Wizard starts. Click **Next**.
9. The next choice is the type of command this taskpad will run. If this taskpad is being used for a simple network task, accept the default menu command. Click **Next**.
10. You can now choose what commands to include in the taskpad. For example, if you want to give the user the task of resetting the password for the user accounts in an OU, verify that **List in details pane** is selected as the command source, and click **Reset Password** in the **Available commands** box. See Figure 4-15. If you want to give a user the task of adding users to an OU, then select **Tree item task** as the command source, and select **New/User** from the available commands. Once you have made your selection, click **Next**.



**Figure 4-15** Choosing commands for the Taskpad

11. Type a task name and description. Click **Next**.
12. Select an icon for the task. Click **Next**.
13. If you want to assign another task, select the **Run this wizard again** check box. Click **Finish**.
14. The taskpad that you just created now appears in the details pane in the MMC. If you want only the taskpad to be visible, then click **View/Customize** and clear all of the check marks for what is visible.
15. Click **Console/Options** and set the mode to **User mode – limited access, single window**. Check the option to not save changes, and remove the check marks for enabling context menus and allowing the user to customize views. Click **OK**.
16. Save the MMC and set the NTFS permissions to read-only.
17. When the taskpad is opened, only the taskpad with its icons and lists is visible. See Figure 4-16 for an example.



**Figure 4-16** A sample Taskpad

## Designing Active Directory for Delegation

When a new domain is created, a domain local group called Administrators is also created on the Domain Controller. This group, which includes the local Administrator account, the Domain Admins global group, and the Enterprise Admins global group from the tree root domain, has full control over all objects in the domain. This group is also the only group that can add additional Domain Controllers to the domain and create OUs. In addition, the Administrators group has the right to take ownership of any object in the domain and to always retain full control of the object, regardless of what permissions have been set.

The Administrators group should be used to administer the top level of the domain. That means that a member of this group implements the original OU structure and retains full control of the upper-level OUs. The authority that this group has requires that the membership of this group be strictly controlled and carefully planned. (Review Securing Active Directory earlier in this chapter for information regarding Restricted Groups.)

In most cases, the members of the Administrators group implement the delegation of administrative permissions. They create the first-level OUs and then assign the administrative delegation that best suits the needs of those OUs. For example, if an OU is in a remote location with local administrators, full control of the OU may be delegated to those administrators. In other OUs, more limited permissions may be given, such as delegating the right to create users. These permissions can be limited even more, to the extent that you can give a user or group the right to change a single property on an object. For example, the Human Resource (HR) department is given the task of ensuring that the phone number and address information is accurate for all users. The

HR department can be given the right to change these properties on all users without giving them the right to modify any other attributes.

Most delegation takes place at the OU level. However, permissions can also be delegated at a site level or domain level. By assigning permissions at a site level and using the inheritance of permissions, you can give a group control over all OUs in that site, which usually corresponds to a physical location for the company. Domain-level delegation is almost always used for one of two purposes: assigning a user the right to add computers to the domain, or assigning the right to work with domain-level group policies.

## Delegating Full Control

In some cases, the best option for a particular OU is to assign full control of that container to a group. For example, Lonestar Graphics may create a special division within the company that handles the creation and publication of specialized brochures. This division may be located in a separate office and may operate almost autonomously. The central IT team can create a separate OU for the division and assign one person or group as the administrator for that OU. This administrator should have full control of the OU in order to create users, add computers, create shares, assign group policies, and possibly even create additional child OUs. At the same time, that local administrator should have control of only that OU and not be able to administer any objects in the rest of the domain.

The domain administrator can create the OU and then create a domain local group that will be given full control of the OU. Then, using the DACL on the OU or the Delegation of Administration Wizard, the administrator can give this group full control of the OU. The administrator would also place a global group into the domain local group, which contains the user accounts of any user that is to be given administrative access to the OU.



Be sure that the domain local and global groups are created outside of the OU. This will ensure that only higher administrators can edit the group memberships.

## Delegating Partial Control

In other situations, the domain administrators may decide to delegate some administrative permissions to another user or group, but not give the user full control of an OU. For example, a number of new computers may be installed in an office, and the administrators may want to give the technician that is doing the installation the right to add computers to the domain, but not to do anything else. The delegation of partial control usually consists of one of two types:

- *Delegating control of an object class*—When you delegate control of an object class, you are giving a user the permission to manage objects of a certain class.

For example, you may give an administrator the right to add, remove, and change the properties of user accounts. Or you may delegate the administration of group accounts.

- *Delegating control of an object attribute*—You can delegate administrative control of a single attribute for an object. For example, you can give a user the right to reset passwords for users in a particular OU. This can be a very useful delegation, because you can give one person the right to reset the passwords for all other people in a department. This user, who will usually be in the same department as the other users, can provide a very useful service, while freeing domain administrators to do the more complex domain administrative tasks.

---

## IMPLEMENTING SECURITY GROUPS

Another essential component of your security plan is a plan for the implementation of security groups. Security groups are used in a variety of ways throughout the network infrastructure. From a user management perspective, security groups give an administrator the ability to quickly assign and control resource access to a large number of users. From an administrative standpoint, security groups can be used to delegate and partition administrative tasks within the Active Directory.

As you work with security groups, you need to keep in mind the distinction between security groups and organizational units. In the past, Windows NT used groups to organize users into various departments, which in turn were used to apply permissions to resources. Organizational units are also used to organize objects into various departments, but cannot be used to assign permissions to resources. Organizational units are not security principals. In Windows 2000, like Windows NT, security groups are still used to assign permissions to network resources or delegate administrative tasks.

### Group Types and Scopes

There are two types of groups available in Windows 2000:

- **Security groups**—Used to assign permission to objects in Active Directory. Any security principal, including other groups, can be added to security groups.
- **Distribution groups**—Used to group users together for specific purposes, primarily e-mail distribution lists, but cannot be used to assign permissions to objects. Any security groups can be added to distribution groups, but distribution groups cannot be added to security groups. Distribution groups are not security principals.

When planning the security policy, you will work primarily with security groups. Security groups can be defined with four different scopes (as listed in Table 4-4). The scope of a group determines who can belong to a group, as well as where that group can be used to grant permissions.

Table 4-4 Security group scopes

Group Scope	Group Members	Access Resources
Computer local group	Can contain any local or domain user accounts and global groups from any domain.	Can be used to assign permissions only to resources on the computer in which the group resides.
Domain local group	Can contain user accounts, global group accounts, universal group accounts from any domain in the forest, and other domain local groups in the local domain.	Can be used to assign permissions only in the domain where the group is located. These groups do not get replicated to the Global Catalog and are not visible outside the domain.
Global groups	Can contain user accounts and global groups from the same domain.	Can be used to assign permissions anywhere in the forest. These groups are listed in the Global Catalog, but the group membership is not.
Universal groups	Can contain user accounts, global group accounts, and universal group accounts from any domain in the forest.	Can be used to assign permissions anywhere in the forest. These groups and the members of the groups are listed in the Global Catalog.



The above descriptions only apply if the domain has been switched to native mode. While the domain is running in mixed mode, universal groups are not available at all, and you also lose the option to nest groups. That is, you cannot add groups to the same type of groups. For example, in a mixed mode domain, you cannot add a global group to a global group, or a domain local group to a domain local group. Another distinction between native and mixed mode domains has to do with how domain local groups are used. In a mixed mode domain, domain local groups can be used to assign permissions only on Domain Controllers. In a native mode domain, domain local groups can be used to assign permissions on any member server in the domain.

Windows 2000 also allows for the option of converting groups from one scope to another, as long as scope rules are not violated. For example, if a domain local group consists of another nested domain local group, it cannot be converted to a Universal group, because a Universal group cannot contain a domain local group.

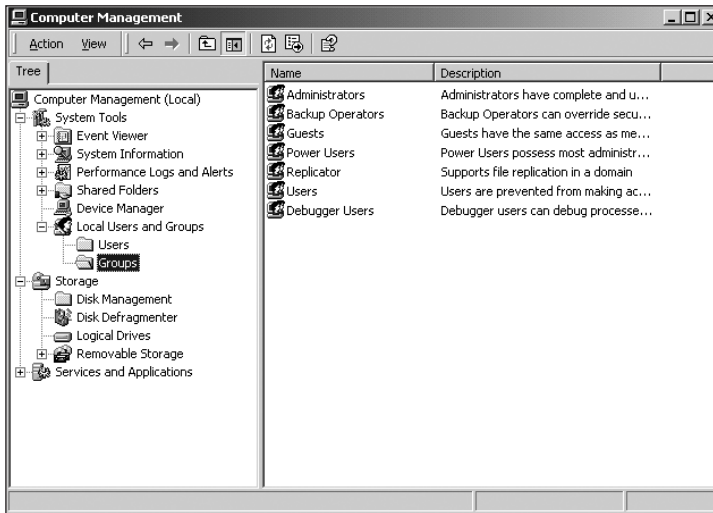
## Default and Built-in Groups

There are a number of built-in security groups with various preassigned rights, which may meet the requirements of the organization's security policy. Whenever possible, you should use one of the built-in groups to assign permissions, because this eases the implementation of delegation and security rights throughout the network. For example,



rather than creating a special group with permissions to back up and restore servers, you can use the built-in Backup Operators group.

Windows 2000 Professional and standalone servers have built-in local groups that provide certain rights on the local machine. These can be found within the Computer Management MMC in the Local Users and Groups node. See Figure 4-17.



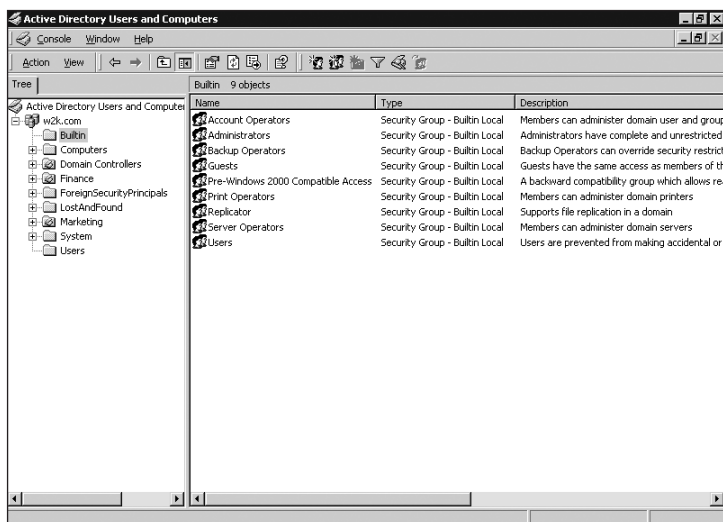
**Figure 4-17** Built-in groups on a local machine

The following table illustrates the types of local groups available on a workstation or standalone server and the rights assigned to each.

**Table 4-5** Local groups and their rights

Group Type	Right
Administrators	Assigned complete unrestricted access to the local computer and possibly the domain.
Power Users	Have the ability to install software, create local users and groups, create and delete nonadministrative shares, change system time, change display settings, and administer local printers.
Backup Operators	Have the ability to override security restrictions for the purpose of backing up or restoring files.
Guests	Have no default permissions or rights. NOTE: The Guests group is a member of the special group Everyone. This means that any access permissions given to the Everyone group give permissions to the Guests group.
Replicator	Used by the File Replication Service.
Users	Have no default permissions, except for permissions assigned by the administrator.

Domain Controllers have a few more domain local groups. These groups are found in the Built-in folder within Active Directory Users and Computers MMC. See Figure 4-18.



**Figure 4-18** Active Directory Built-in group

**Table 4-6** Built-in groups and their rights

Group Type	Right
Account Operators	Have the ability to create, delete, and modify user accounts and groups within the domain. They cannot place themselves or anyone else in the Administrators group.
Pre-Windows 2000 Compatible Access	This group is created to support applications that work with Windows NT 4.0, but may have problems with Windows 2000 security. This group has read access on all users and groups within the domain. This is used primarily for Windows NT RAS servers that require access to Active Directory.
Print Operators	Members of this group have all print administration rights.
Server Operators	Members of this group can share disk resources, back up and restore files, and shut down or restart the server.

The Users container in Active Directory Users and Computers also contains various global groups that can be used throughout the domain. See Figure 4-19. Notice that some of the global groups, such as Domain Controllers, contain computer objects as opposed to user objects.

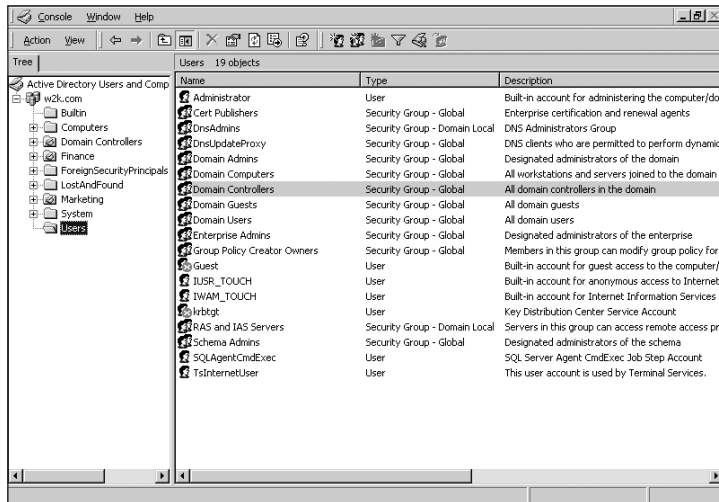


Figure 4-19 Active Directory Users container

## Managing Security Groups

As you design your security plan, you can use the enhanced options with Active Directory groups to plan the assignment of permissions based on groups. A general strategy is to use the common acronym, A G U DL P. This refers to:

1. Create user **A**ccounts, and organize them within **G**lobal groups. Often users are grouped in global groups based on departments in the organization.
2. Optional: Create **U**niversal groups and place Global groups within the Universal groups.
3. Create **D**omain **L**ocal groups that represent different levels of access to each resource and add the Global or Universal groups to the domain local groups.
4. Assign **P**ermissions to the domain local groups.

If your domain is running in native mode, you can use the option of nesting groups to simplify administrative tasks. For example, Lonestar Publishing may have three groups called Agents, Marketing, and Distributors. Together, these three groups of users may represent the Customer Service component of Lonestar Publishing. You could create the CustServ group and put all three groups into this one group, thus simplifying the assignment of permissions for resources to which all three groups should have access. You do not need to add individuals to the CustServ group. When you are assigning permissions to resources, assign the permissions to domain local groups.

If you are working in a single domain and a single site, you can use Global groups or universal groups interchangeably. Choose one of these options to group your users and then add these groups to the local domain groups. If you are working in an organization

with multiple sites separated by slow network links, the use of universal groups and global groups must be carefully planned. One of the goals in this type of network configuration is to minimize the network traffic across the slow network links. A global group is listed in global catalog, but its membership is not. Therefore, if a member is added to a global group, no replication traffic is created between global catalog servers. A Universal group is also listed in the global catalog, but the membership of the group is included. If you add a member to a Universal group, the new membership information is replicated to all global catalog servers. The advantage of using Universal groups in a multi-domain environment is that the members of a Universal group can come from any domain in the forest, and the Universal group can be used to assign permissions to any resource in the tree. However, if you have large Universal groups, the replication traffic between global catalog servers can be significant, especially across slow WAN links.

The following example shows how you can use Universal groups and Global groups. Lonestar Publishing has an Agents share resource located at head office that all agents should be able to access, regardless of which domain they are in. To allow this, you can create a Universal group, add all of the Agents Global groups from the different domains to that one Universal group, and then assign that Universal group to a local domain group that has permission to access the Agents share. To combine the benefits of using universal groups with the limitations imposed by slow network links, always assign Global groups to Universal groups, rather than assigning individual user accounts to the Universal group. The Universal group membership is still replicated to all global catalog servers. However, if the membership consists only of Global groups, the membership information rarely changes, resulting in very little replication traffic.

---

## IMPLEMENTING GROUP POLICIES FOR SECURITY


Another of the important improvements of Windows 2000 Active Directory over Windows NT domains is the option to use group policies. Group policies are powerful administrative tools that can be used to do a variety of administrative tasks, including automation of software installation on computers throughout the network, configuration of desktop settings, and setting restrictions on the changes users can make to their computers. Your security plan will need to include a description of how you intend to use group policies to administer security on your network.

### Group Policy Overview

**Group Policy** enables the centralized management of user and computer settings throughout your network. With group policies, you can configure various security policies on the domain controller and then rely on the server to enforce those policies for all users and computers that are part of your domain.

To implement group policies, you must first define the group policy or use and modify one of the default group policies to meet the company requirements. Then, you can link

the Group Policy to a site, a domain, or an organizational unit. When you link the group policy to one of these container objects, the Group Policy settings will be applied to all users and Windows 2000 computers in the container.



Group Policy can be applied only to Windows 2000-based computers. If you still have down-level clients such as Windows NT or Windows 9x, you must use system policies.

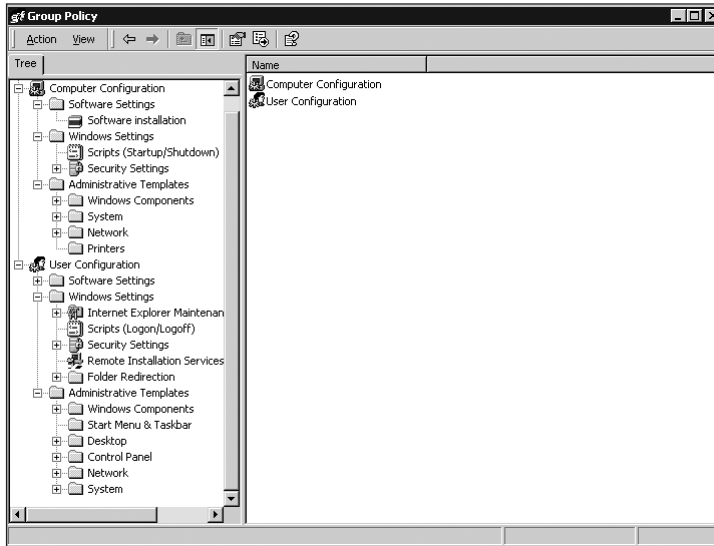
## Group Policy Configuration Options

Group Policy can apply a variety of configuration options to the local computer, site, domain, and organizational unit. There are two main categories to a Group Policy: a computer category and a user category. Any configuration settings set within the computer category will affect computers located in the container that the Group Policy Object (GPO) is linked to. The user category is similar in that any configuration settings set within this category will apply to any users with accounts in the container.

Table 4-7 lists the categories available under both computer and user configuration. Figure 4-20 illustrates the interface used to administer Group Policies.

**Table 4-7** Configuration options available in Group Policies

Configuration Options	Explanation
Software Settings	Used to centralize the management of software installation and maintenance. The installation, upgrading, and removal of applications can be controlled from one central location.
Windows Settings	Used to manage the deployment and management of scripts, security settings, Internet Explorer settings, and features, such as Remote Installation Services and Folder Redirection.
Administrative Templates	Used to set registry-based settings to configure application and user desktop settings. This includes access to the operating system components, access to Control Panel settings, and configuration of offline files.



**Figure 4-20** Default domain controllers Group Policy

## Group Policy Objects

Group Policies are implemented by using GPOs. To implement a Group Policy, first create a GPO, and then associate it with a container object in Active Directory.

GPO content is actually stored in two different locations on the server.

- **Group Policy Container**—An Active Directory container that stores information about the GPO and includes a version number that is used by other domain controllers to ensure that they have the latest information. The version number is also used to make sure that the Group Policy Template (GPT) is synchronized. The GPC is located in Active Directory Users and Computers, System, Policies.
- **Group Policy Template**—Contains the actual data that makes up the Group Policy. The template includes all the settings, the administrative templates, security settings, software installation settings, scripts, etc. The actual registry changes are stored in a configuration file named **Registry.pol**. A configuration file is stored for both the user settings and computer settings. The GPT is stored in the %systemroot%\Sysvol\Sysvol folder.

Both the GPC and the GPT are identified by a globally unique identifier (GUID), which is a unique 128-bit number assigned to the object when it is created. GUIDs are guaranteed to be unique for the entire forest. When a computer accesses the GPO, it uses the GUID to distinguish between group policies.

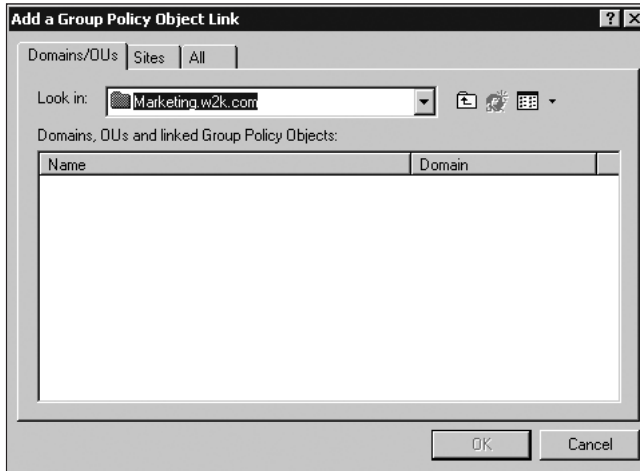
## Managing Group Policies

Group Policies can be linked to site, domain, or OU containers in Active Directory. This allows the administrator to use maximum flexibility when applying Group Policies in the network. There are a number of possibilities.

- If you have a set of Group Policies that need to be applied to all users in a particular location, apply the Group Policy at the site level. You might also choose to apply Group Policies at domain level if the policies need to apply to all domain users. Some policies, such as password and account policies, can only be applied at a domain level. Other policies may affect only a small group of users. In this case, put all the users in the same OU, and then apply the group policy at the OU level.
- You can have multiple Group Policies assigned to one container. You may want to create several GPOs that define different settings and then link all of them to a specific container. For example, you may want to create a policy that defines security settings, and another that defines user desktop settings, and then link both of them to the same container.
- You can use the same Group Policy and link it to multiple containers. This allows you to create a policy once and then use that policy for different containers. For example, you may create a policy for software distribution and then link that policy to the OUs where the policy should be applied.

To link Group Policy objects to Active Directory containers, use the following procedure.

1. Click **Active Directory Users and Computers** and right-click the container you want to link to a GPO. (If you are linking a GPO to a site, open Active Directory Sites and Services, and right-click a site.)
2. Click **Properties** and click the **Group Policies** tab.
3. Click **Add** and you will see all of the possible locations where GPOs can be stored. (See Figure 4-21.) If you have created that GPO for another container, browse to that container, select the GPO, and then click **OK**.



**Figure 4-21** Locating Group Policies to link to an Active Directory container

To find out what containers are all linked to a particular GPO:

1. Click the GPO in one of the containers and click **Properties**.
2. Click the **Links** tab to make sure that you are searching for the right container.
3. Click **Find Now**. The list will show all of the containers with links to the GPO.

## Creating Group Policies

Group Policies can be created in two different ways: by using the Group Policy standalone snap-in or by using the Group Policy extension in Active Directory Users and Computers.

To create a new Group Policy using the standalone snap-in, follow the directions below:

1. Create a custom MMC and add the Group Policy snap-in. When you are loading the snap-in, you can choose the policy you want to administer. Click **Browse**.
2. You can now browse for any already existing Group Policy to edit, or you can create a new Group Policy by clicking on the **New Policy** icon. Type the name of the Group Policy and click **OK**.
3. Return to the console root and edit the policy to match your needs.
4. When you have finished editing the policy, you can apply it to any container in Active Directory.

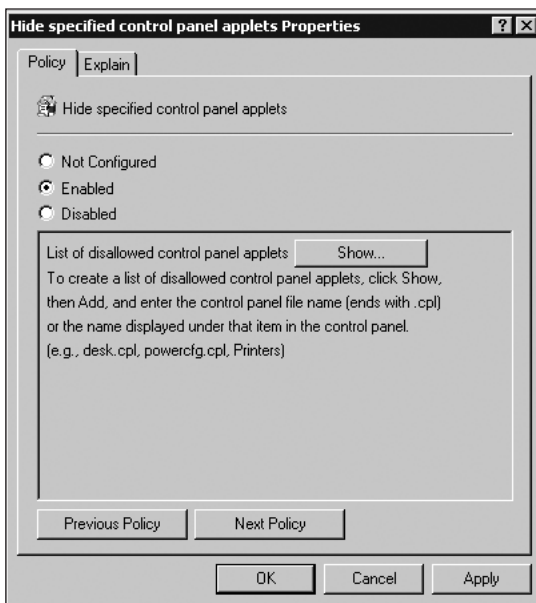


To create a new Group Policy using the Group Policy Extension, follow the directions below:

1. Click **Active Directory Users and Computers** and right-click the container object where you want to create the new policy.
2. Click **Properties**, and then click the **Group Policy** tab.
3. Click **New** and type in the name for the policy.
4. To edit the policy, select the policy in the window and click **Edit**.

When you create a new policy using either method, the Group Policy loads a template that includes all of the options listed. You can edit the template or create a new one.

When you are editing a policy and want to enable a particular setting, right-click the setting and click Properties. Figure 4-22 shows the properties of the option to Hide specified control panel applets. The Policy tab allows you to enable or disable the setting, as well as set any parameters that may be needed. The Explain tab provides information on what the effect of applying that setting will be.



**Figure 4-22** Enabling or disabling Group Policy settings

## Application of Group Policy

Group Policies are applied when a computer starts or when a user logs on. However, because Group Policies can be applied at the site, domain, or OU level, one computer

could process multiple policies during the startup and logon process. Group Policies are applied in the following order:

1. Local Computer
2. Site
3. Domain
4. Parent OU
5. Child OU

At each level, more than one GPO can be applied. If there is more than one GPO per container, the policies are applied in the order that they appear on the Group Policy tab for the container, starting with the bottom GPO first.

All of the Group Policies settings are inherited. For example, a Group Policy setting on a parent container will also be applied to the child containers, and therefore to all the users and computers in the child containers. One computer or user could be processing many policies during startup and logon.

When a computer is started and a user logs on, the following process takes place:

1. A Windows 2000 client computer in a domain starts up. The client computer queries the Domain Controller for a list of GPOs that it needs to apply. The Domain Controller examines all of the GPOs to see which policies apply to the computer. Policies that are executed on the computer include the computer settings and startup scripts.
2. The Domain Controller presents the client with the list of GPOs that apply to it in the order that the GPOs need to be processed. The computer contacts the Domain Controller, extracts the Group Policies templates from the Sysvol share, applies the settings, and runs the scripts.
3. When the user logs on, the same process happens again, except this time the user settings, logon scripts, software policies, etc., are applied.

After a user has logged on, the computer will refresh its policies every 90 minutes (plus an added random time up to 30 minutes, which varies by computer, so that all the computers don't contact the Domain Controller to refresh at the same time). If a user does not shut down his computer, or a setting has changed in the Group Policy, then refreshing the policy makes sure that the computer and user settings are up to date. Domain Controllers and member servers refresh their Group Policy settings every five minutes.

## Group Policy Conflicts

Because of the multiple policies that can be applied to a user or computer, there is the chance that there will be a conflict in the settings between policies. The computer uses the following steps to determine which policy to apply.

1. If there is no conflict, then both policies are applied. For example, if a policy at a domain level enables a certain setting, and the policy at an OU level has that setting set as Not Configured, then the domain policy will be applied.
2. If there is a conflict, then later settings overwrite earlier settings. If both a domain-level policy and an OU-level policy configure the same setting differently, then the OU-level policy will be applied.
3. Computer policies will usually overwrite user policies.

To understand this process, look at the following example of how a policy setting would be enforced for a user whose account is located in the Managers OU, which is a child OU to the Administration OU. The Administration OU is located in the Widgets.com domain, in the Default-First-Site-Name site.

**Table 4-8** Options for enforcing policy settings

Container	GPO setting
Default-First-Site-Name	Restricts the user from using author mode when using customized MMCs.
Widgets.com	Password length must be at least 8 characters. Removes the Run command from the Start menu.
Administration OU	Disables the Control Panel. Adds the Run command to the Start menu.
Managers OU	Allows the user to use author mode in MMC. Password length must be at least 10 characters.

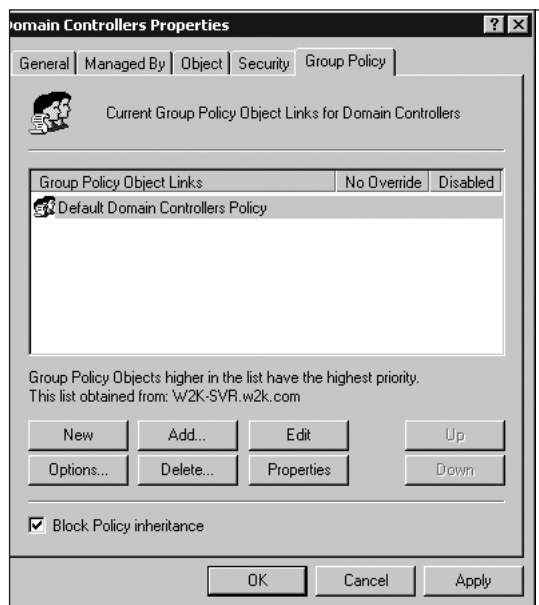
What settings will be set for this user?

- Will be able to run MMC in author mode.
- Control Panel will be disabled.
- Run command will be visible.
- Password length will be 8 characters—the password length can be set only at the domain level.

## Administering Group Policy Inheritance

By default, all Group Policy settings are inherited from parent containers. However, there are several ways to change this default behavior.

**Blocking Group Policy Settings**—If you do not want any of the higher-level settings to be applied to a particular child container, then check the Block Policy inheritance option on the Group Policy tab for the container properties. Figure 4-23 shows the interface.



**Figure 4-23** Blocking Group Policy inheritance

Selecting the option to block policy inheritance means that all policies from parent containers will be blocked. Individual Group Policies from parent containers cannot be blocked. In addition, Group Policies that are set to no override from a parent container will not be blocked.

Blocking Group Policies can be very useful if you have one OU that has very different policy requirements than all of the other OUs, or if the OU must be separately managed.

**Forcing Group Policy Settings**—If you want a particular group policy to always be enforced, then you can force a group policy by selecting Options for a particular group policy, and then selecting No Override.



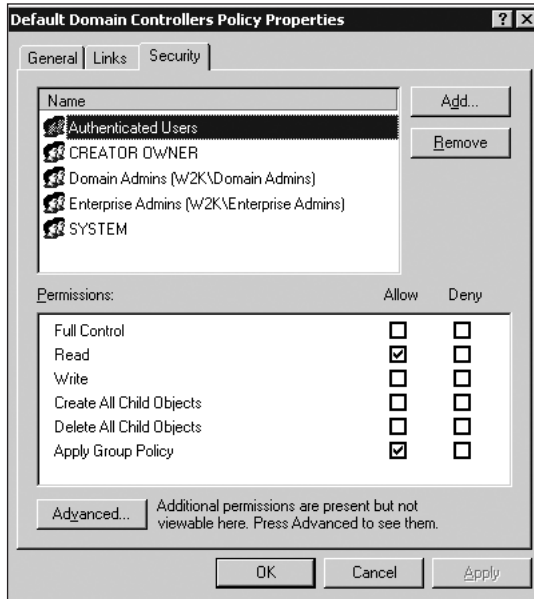
**Figure 4-24** No override option in Group Policy

This will result in the policy's being enforced, even if a lower-level policy that is processed later tries to change a setting. The No Override setting will also enforce a policy on a container that has the Block Policy Inheritance set. Use this option if there is a particular group of settings that must be enforced in your entire network, and then link this policy to the domain or site level so that it will apply to all containers.

*Filtering Group Policy Settings*—The third way of affecting the inheritance of Group Policies is used to prevent Group Policy settings from applying to a particular user, group, or computer within a container. For example, the Managers OU may have a GPO linked to it, but you don't want the settings from the GPO to apply to the General Manager. To filter the General Manager so that he does not have the GPO applied:

1. Click the **Group Policy** tab, click the GPO that you are configuring, and then click **Properties**.
2. Click the **Security** tab. Figure 4-25 shows the interface.
3. Choose or add the user, group, or computer that you want to filter out, and then clear the **Apply Group Policy** and **Read** permissions.

This will now prevent this Group Policy from being applied to that user or group.



**Figure 4-25** Group Policy Security tab

## Troubleshooting Group Policy Settings

There may be times when Group Policy does not work as expected. Restrictions may not be enforced as configured or may be too restricted and interfere with user productivity.

A careful inspection of the Active Directory hierarchy will possibly uncover the reasons for Group Policy not working the way it should. Be sure to inspect all containers above and below the OU that is causing the problem. In some cases, improper use of No Override or Block Policy inheritance settings can cause problems. Another area to be aware of is the Group Policy's Security tab. Make sure that the user or group has been assigned the Read Group Policy and Apply Group Policy permissions.

The administrator can also use a utility from the Windows 2000 Resource Kit called Gpresult. This utility is handy in that it can be used to discover Group Policy-related problems and illustrates which Group Policy objects were applied to a user or computer. Gpresult will also list all group memberships of the user or computer being analyzed.

To use the utility, it must be run on the computer where the user logs on. Gpresult uses the following syntax:

```
Gpresult [/V] [/S] [/C] [/U] [/?]  
/V—verbose mode  
/S—super verbose mode
```

/C—shows only Group Policy objects applied to the computer  
 /U—shows only Group Policy objects applied to the user

## PLANNING BEST PRACTICES

- Be sure to use NTFS as the standard file system throughout the organization. Security templates may not be as effective as expected without NTFS.
- Place all computers that require a specific security template within the same OU. This will minimize the amount of links and applications of the Group Policy object.
- Be sure to test all Group Policy objects before deploying them into a production environment.
- Set a Minimum Password Age to stop users from cycling through and reusing a recent password.
- Take advantage of the Restricted Groups feature of the security policy to ensure that groups have only authorized users as members.
- Separate the Backup group into two custom groups. One group can be for backup and the other for restore purposes. This will increase security because anyone who can back up data will not be able to restore the information without involving someone from the other group.
- Use the Delegation of Control Wizard to delegate special tasks to nonadministrators, such as resetting of locked accounts.
- Remember that Account Policies can be applied only at the domain level.
- Do not add user account names to a Universal group. Be sure to include only Global groups within Universal groups.
- Minimize the number of levels applied to Group Policy. The more Group Policies that are applied, the slower the logon process will be.

## CHAPTER SUMMARY

- Active Directory consists of four logical components: forests, domains, trees, and organizational units. Forests are a collection of domains that do not share a contiguous naming convention. Domains are a collection of objects sharing the same directory database. Trees include one or more domains that are hierarchically structured and share a common DNS name. Organizational units are used to organize common departments or geographical locations into groups within the Active Directory.

- Security Templates can be used to quickly apply and maintain security settings on Windows 2000 computers. These templates are text files that can be saved and reapplied when necessary.
- The Security Configuration and Analysis Utility can be used to compare a computer's current security settings to a previously configured template. This utility can also create, modify, and apply security templates to a particular computer.
- One of the most common configuration categories that administrators will adjust is the Account Policies. Account Policies include such settings as password policies, lockout policies, and Kerberos ticket policies.
- Active Directory provides the capability for easy delegation of administrative duties. The easiest way to delegate an administrative task is to use the Delegation of Control Wizard. This wizard will allow the administrator to choose the user or group, and the task that is to be delegated.
- Windows 2000 now incorporates four main security groups to be used within the network system: Computer Local Groups, Domain Local Groups, Global Groups, and Universal Groups. The use of Universal Groups requires that the domain be in native mode.
- Windows 2000 includes a new feature called Group Policy, which allows the administrator to centrally administer and apply various enterprise-wide settings, such as security settings, application deployment, and administrative templates.

---

## KEY TERMS

**Active Directory** — The directory service in Windows 2000.

**Active Directory schema** — A list of object classes and attribute classes available in Active Directory.

**Active Directory Tree** — A grouping of one or more Windows 2000 domains.

**child domain** — A domain that is connected to another parent domain in an Active Directory tree. The child domain shares a contiguous DNS namespace with the parent domain.

**Computer Local group** — A group that resides in the local directory database of a workstation or standalone server.

**delegation** — The process of distributing and decentralizing the administration of Active Directory.

**directory service** — A central database that stores information about network-based objects such as computers, printers, users, and groups.



**Distribution group** — A group that is used to organize users for specific tasks like sending batch e-mail messages.

**domain** — A collections of objects that share the same user account database and security policy.

**domain local group** — A group of common objects created on a domain controller and used to control permissions for resource access.

**forest** — A collection of Active Directory Trees connected by trust relationships. The trees in a forest do not share a contiguous namespace.

**Global group** — A security group used to create collections of users or computers.

**global catalog** — A subset and collection of attributes from every object within the forest.

**Group Policy** — An object created that allows centralized management of user and computer configuration settings.

**organizational unit (OU)** — A grouping of common objects, such as users and groups, that all share the same departmental and security policies.

**root domain** — The first domain installed in an Active Directory structure.

**secedit.exe** — A command-line tool used to analyze and configure security templates.

**Security and Configuration tool set** — A set of tools that help create, analyze, and apply security template configurations.

**Security group** — A group of security principals collected for the purpose of applying specific permissions to resources.

**Security Policy Template** — A file that contains a collection of security settings that can be applied to users or computers by using the Security Configuration Tool set.

**transitive trust** — The link between domains in Active Directory.

**Universal group** — A collection of objects that can be assigned permissions throughout the entire Active Directory Forest.

---

## REVIEW QUESTIONS

1. Which type of security group has its entire membership stored in the Global Catalog?
  - a. Domain Local groups
  - b. Universal groups
  - c. Local Computer groups
  - d. Global groups
  - e. all of the above

2. What type of trust is created between a Windows 2000 domain and a Windows NT-based domain or a Windows 2000 domain in another forest?
  - a. automatic, one-way, non-transitive
  - b. automatic, one-way, transitive
  - c. automatic, two-way, transitive
  - d. explicit, one-way, non-transitive
  - e. explicit, one-way, transitive
  - f. explicit, two-way, non-transitive
3. What type of group is not available for managing user rights and permissions in a mixed mode Windows 2000 domain?
  - a. Universal groups
  - b. Global groups
  - c. Domain Local groups
  - d. Local Computer groups
  - e. Online Users groups
  - f. none of the above
4. You would like to give three users from a trusted domain access to a share in your domain. What type of group must the users belong to in order for you to assign the permission to the group?
  - a. Global group
  - b. Domain Local group
  - c. Local Computer group
  - d. Domain Local or Global group
  - e. any of the above
5. The Enterprise Admins group is:
  - a. located only in the root domain of a forest
  - b. automatically added to the Administrators group in every domain in the Forest
  - c. located in every domain in the forest
  - d. made up of all the Domain Administrators from all the domains in the forest
6. The role of the schema in Windows 2000 Active Directory is to:
  - a. Define what types of objects can be created in the forest.
  - b. Define how many domains can be created in the forest.
  - c. Define what attributes must be assigned a value when creating a user object.
  - d. Allow each domain in the forest to have different class and attribute objects.

7. In an Active Directory forest, the Organizational Unit can be used to:
  - a. define a unique password policy for a group of users.
  - b. block the Domain Admins group from modifying the properties on a user account.
  - c. assign permissions to a network resource.
  - d. group users for administrative purposes.
8. Security Templates are used to:
  - a. configure security settings for all the computers in an OU.
  - b. modify the attributes like address information for a large group of users at one time.
  - c. check the security of your firewall configuration.
  - d. check the security settings for security policies such as password policies.
9. What would be the effect of the following Account Lockout Policy: Account lockout threshold – 5, Account lockout duration – 30, Reset the account lockout counter after – 10?
  - a. A user would be locked out for 10 minutes after five bad logon attempts.
  - b. A user would be locked out for 30 minutes after nine bad logon attempts.
  - c. A user would be locked out for 30 minutes after five bad logon attempts.
  - d. A user would be able to try four times to log on, and then wait 10 minutes and try again without being locked out.
10. Your company is opening an office in a city where you do not currently have an office. You would like to be able to have one of the users in the office do some simple user administration and reset passwords, but the user should not be able to do anything else on your network. What would be the most appropriate configuration option in Active Directory for the users and computers in the office?
  - a. create an OU inside an existing domain.
  - b. create a new domain that is not part of an existing domain tree.
  - c. create a new child domain inside an existing domain tree.
  - d. create a new domain tree inside an existing forest of domain trees.
11. By default, any permissions that are assigned at a domain level in a parent domain are:
  - a. inherited for all objects in the domain and child domains.
  - b. inherited for all objects in the domain.
  - c. inherited for all objects in the domain except for objects placed into an OU.
  - d. not inherited for any objects in the domain.

12. You want to give the help desk personnel the right to reset passwords for all user accounts in your office except for the user accounts for the executives and managers. The easiest way to do this is to:
  - a. give the help desk personnel the right to reset user accounts at the domain level.
  - b. put all the help desk personnel into an OU and assign the OU the right to reset passwords.
  - c. put all the executive and manager accounts into an OU and assign the help desk personnel the reset password permission at the domain level.
  - d. put all the non-executive and non-manager user accounts into an OU and give the help desk personnel the right to reset passwords for the OU.
13. Which feature makes Windows 2000 administration more flexible to manage in a single domain network than Windows NT?
  - a. delegation of administrative authority at an OU level
  - b. auditing
  - c. Kerberos version 5
  - d. automatic trusts between domains in a forest
14. A password policy that is too complex may actually decrease the security of your network. True or False?
15. In order to make a password difficult to guess in a brute force attack, your password should:
  - a. be more than eight characters long
  - b. include your first name as part of the password
  - c. include upper case and lower case characters
  - d. include numbers or special characters
16. You would like to give the Human Resources department the right to manage user objects in one OU in your organization. You create and configure a customized MMC for the HR department so that only that OU is visible in the MMC. You test the MMC and it works perfectly, but when you asked a member of the HR department to test the MMC, they cannot change any settings on the user accounts. Why not?
  - a. The HR department has not been trained to use the MMC.
  - b. You did not grant the HR department the right level of permissions.
  - c. The MMC is configured incorrectly.
  - d. You need to configure a Taskpad to do this.
17. You have created a new group in your domain called Managers and put all of the appropriate users into the group. As well, you have just installed a new file and print server on your network and configured a new Managers share on the server.

- However, when you try to add the Managers group to the NTFS permission on the folder, you cannot locate the group through the interface. What happened?
- The new server has not been added to your domain.
  - You created a distribution group rather than a security group.
  - You created a global group rather than a domain local group.
  - You did not enable the group.
- You have just created a Windows 2000 network with a single domain. You would like to grant the help desk staff the ability to reset user passwords, but not allow them to create and delete user accounts. Can you do this (yes or no)?
  - How would you configure a security policy that would affect all computers in the domain, including Domain Controllers?
    - Edit the local security policy on each computer.
    - Edit the Domain Controllers OU security policy.
    - Edit the domain security policy and confirm that there are no settings in the local security policies that conflict with the domain policy settings.
    - Edit the domain security policy and confirm that there are no settings in the Domain Controllers OU security policy that conflict with the domain policy settings.
  - You decide to implement a group policy that will prevent all users except network support personnel from being able to change their network settings. You configure the domain security policy to meet your requirements, and then notice that even the network support personnel cannot change the network settings on any computers. How could you fix this?
    - Move the network support personnel into a separate OU and block the policy inheritance.
    - Apply the group policy on the User container rather than the domain.
    - You can't do this in Active Directory.
    - Move all of the users other than the network support personnel into a separate OU.

---

## HANDS-ON PROJECTS



### Project 4-1

In this hands-on project you will create a custom Microsoft Management Console and add the Security Templates snap-in.

To create a custom MMC:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Start**, **Run**, and type **mmc** at the command line. Click **OK**.
3. In the Console window, click **Console, Add/Remove Snap-in**.
4. Click the **Add** button and scroll down to select the **Security Templates** snap-in.
5. Click **Add** and then click **OK** to return to the custom MMC dialog box.
6. Maximize the console root window.
7. Click **Console** and then click **Save As**. Name the console **Security Templates** and then click **Save**.
8. Close the **Security Templates** console.
9. Click **Start**, point to **Programs**, and point to **Administrative Tools**. You should see your newly created Security Templates console.
10. Close all windows and log off.



## Project 4-2

In this hands-on project you will create a new security template that will set account policy configurations for the domain.

To create a new security template:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Start**, point to **Programs**, and point to **Administrative Tools**. Click **Security Templates**.
3. Expand the **Security Templates** node. Notice the physical path to the location of the actual template files.
4. Expand the template path node to view the various pre-configured templates.
5. Right-click the template path node, and choose **New Template**. Name the new template **Account Template**. Click **OK**.
6. Expand the **Account Template** node to view the configuration categories.
7. Expand the **Account Policies** node. Configure the following settings:

Password History	4 passwords must be remembered
Maximum Password Age	30 days
Minimum Password Length	7 characters
Account Lockout Duration	Administrator must unlock account
Account Lockout Threshold	Account locks out after 4 attempts
Account Lockout Counter	30 Minutes

8. Right-click **Account Template** and choose **Save**.

9. Close all windows. Click **Yes** to save the console settings.
10. Log off.



## Project 4-3

In this hands-on project you will create another new MMC console with the Security Configuration and Analysis snap-in added. You will then use the console to analyze and compare the Account Template configurations to the local computer.

1. Log on to your Windows 2000 computer as an administrator.
2. Create another MMC console with the **Security Configuration and Analysis** snap-in added. (If you forget how to create an MMC console, see Project 4-1.)
3. Save the new console with the name **Security Analysis**.
4. To analyze a security template, in the left pane, select the **Security Configuration and Analysis** node. Read the instructions that appear in the details pane.
5. Right-click **Security Configuration and Analysis** and click **Open Database**.
6. In the filename box, type **Policy** and then click **Open**.
7. On the **Import Template** screen, select the **Account Template** file and then click **Open**. Read the directions that appear in the details pane.
8. Right-click **Security Configuration and Analysis** and click **Analyze Computer Now**.
9. Click **OK** to accept the log file path.
10. Expand the **Account Policies** node. Click the **Password Policy** and **Account Lockout Policy** to view the configuration differences between the local computer and the Account Template file. All differences will have a red X indicating that the template and computer settings are not the same.



## Project 4-4

In this hands-on project, you will apply the configuration settings of the new **Account Template** file using the **Security Analysis** console created in Project 4-3.

To configure a computer to use a custom template:

1. Right-click the **Security Configuration and Analysis** node in the left pane.
2. Click **Configure computer now**.
3. Click **OK** to accept the default path for the log file.
4. To view the changes, right-click **Security Configuration and Analysis** and click **Analyze Computer Now**.
5. Click **OK** to accept the log file path.

6. Expand the **Account Policies** node. Click the **Password Policy** and **Account Lockout Policy** to view the configuration differences between the local computer and the Account Template file. All configurations should have a green check mark next to them to indicate that they are the same.
7. Close and save all windows, and reboot the computer.



## Project 4-5

In this hands-on project, you will test the account lockout policy by attempting to log on with the wrong password.

To test the account policies:

1. At the logon prompt, attempt to logon with the username **bill** and the password **1234**. Click **OK** at the logon message.
2. Attempt the logon four more times. What does the logon message change to after the fourth attempt? Why does this message appear?
3. Log on as the administrator.
4. To unlock Bill's account, open **Active Directory Users and Computers**.
5. Expand the **Lonestar** domain and click the **Users** container.
6. Right-click **Bill Johnson** and click **Properties**.
7. Click the **Account** tab, and deselect the check box next to **Account is locked out**. Click **OK**.
8. Right-click **Bill Johnson** and click **Reset Password**.
9. Enter **1234** as the password and click **OK**. Note the error message you receive when the password is too short. Click **OK** to clear the error.
10. Right-click **Bill Johnson** and click **Reset Password**.
11. Enter **12345678** as the password and click **OK**. Note that the password has been successfully changed. Click **OK** to clear the message.
12. Close all windows and log off.



## Project 4-6

In this hands-on project, you will delegate authority to a junior administrator to be able to manage users in a specific department. This involves creating an OU for the department, adding a user account for the junior administrator to the OU, and then delegating authority of the OU to the junior administrator.

To create a new organizational unit:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.



3. In the left pane, right-click the **Lonestar.com** domain, point to **New**, and click **Organizational Unit**.
4. Enter **Finance** as the name of the OU and click **OK**.
5. To delegate control of the Finance OU, right-click the **Finance** OU, point to **New**, and click **User**.
6. Name the new user **Susan Wright**.
7. Enter **Susan** as the logon name. Click **Next**.
8. Enter a password and click **Next**. Click **Finish**.
9. Right-click the **Finance** OU, and click **Delegate Control**.
10. At the welcome screen, click **Next**.
11. On the Users and Groups screen, click **Add**.
12. Double-click **Susan Wright** and click **OK**. Click **Next**.
13. Click the checkbox for **Create, delete, and manage user accounts**. Click **Next** and then click **Finish**.
14. Close all windows and log off.
15. Test the delegation rights applied to Susan by testing her ability to create new user accounts when she logs in as Susan.
16. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
17. Right-click **Finance**, point to **New**, and click **User**. Create a new user **Jimmy Kent** with a logon name of **Jimmy**. Click **Next**.
18. Enter a password and click **Next** and then click **Finish**.
19. Right-click the **Users** container. Why is there no option to create new users at this container?
20. Close all windows and log off.



## Project 4-7

In this hands-on project, you will create a Global security group called **Finance Admins** and add **Susan Wright** to this group.

To create a Global security group:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
3. Right-click the **Finance** OU, and click **New, Group**.
4. Name the group **Finance Admins**. Click **OK**.
5. Right-click **Susan Wright** and click **Add members to a group**.

6. Select the **Finance Admins** group and click **OK**.
7. Click **OK** in the message box.
8. To verify that Susan was added to the group, double-click **Finance Admins** group and click the **Members** tab. Susan's name should be listed as a member. Click **OK**.
9. Close all windows and log off.



## Project 4-8

In this hands-on project, you will create a Group Policy object that will remove the run command from all users in the Finance OU. The Finance Admins group should not have this policy applied.

To create the Group Policy Object:

1. Log on to your Windows 2000 computer as an administrator.
2. Click **Start**, point to **Programs**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.
3. Right-click the **Finance** OU, and click **Properties**.
4. Click the **Group Policy** tab and click the **New** button.
5. Name the new Group Policy Object **Remove Run Command**.
6. Click the **Remove Run Command** object and click **Edit**.
7. Under the **User Configuration** container, expand **Administrative Templates**.
8. Click the **Start Menu & Taskbar** node.
9. In the details pane, double-click **Remove Run menu from Start Menu**.
10. Click the **Enabled** radio button and click **OK**.
11. Close the Group Policy window.
12. To filter the Finance Admins from getting the policy, click the **Remove run command** Group Policy and click **Properties**.
13. Click the **Security** tab. Click **Add**.
14. Double-click the **Finance Admins** group and click **OK**.
15. With Finance Admins selected, set the **Apply Group Policy** permission to **Deny**. Click **OK** and **Yes** at the Security warning.
16. Close all windows and log off.
17. To test the Group Policy settings, log on as Jimmy Kent. Do you have the run command? Why or why not?
18. Log on as Susan Wright. Do you have the run command? Why or why not?
19. Close all windows and log off.

## CASE PROJECTS



### Case Project 4-1

Southdale Property Management is configured as a single Windows 2000 domain. At this point, all of the user accounts are still located in the Users container where the accounts were created when the Windows NT domain was upgraded to Active Directory. As a result of the security analysis that you have completed, you have decided that you would like to implement the following changes:

- A part-time network administrator should be able to reset the passwords for all accounts except the Administrator account and the managers' accounts.
- You would like to have everyone change their passwords at least once every two months and would like to enforce a policy that would make the user passwords hard to guess.
- You are concerned about people trying to guess each others passwords and so would like to make sure that people cannot keep trying to log on by guessing passwords.
- No one except the network administrators should be able to log on to any of the servers
  1. How would you configure Active Directory to ensure that these requirements are met?
  2. What other Active Directory-related issues should be included in your security planning?



### Case Project 4-2

Fleetwood Credit Union is running a single Active Directory domain with multiple OUs configured for each location. At this point, the company has not implemented any group policies, but they would like to use group policies to implement the following requirements.

- All users should be required to change their passwords at least every 30 days.
- Each office has an administrative assistant that should be able to reset passwords and change the public information, such as phone numbers and departments, for users in that office. The assistant in each office should not be able to modify user attributes for users in any other office. You also need to implement this with as little training as possible for the administrative assistants.
- The Windows 2000 servers must be as secure as possible. Ideally, you should be able to configure the security on the server and then not have to continually monitor the servers to make sure the security configurations have not changed.

- You would like to restrict the user desktops for all the users currently running Windows 2000 Professional. You want to remove the Run command, disable the Control Panel, and disable the registry editing tools on all computers, except when a network administrator logs on to the computer. The network administrators should have access to all these tools regardless of which computer they log onto.
  1. How would you implement these security options using Group Policies?